



Cisco Aironet Access Point Software Configuration Guide

340 and 350 Series
Software Release 12.01T

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-0657-07



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

Cisco Aironet Access Point Software Configuration Guide

Copyright © 2002, Cisco Systems, Inc.

All rights reserved.



Preface xv

Audience and Scope xvi

Organization xvi

Conventions xvii

Related Publications xviii

Obtaining Documentation xix

World Wide Web xix

Documentation CD-ROM xix

Ordering Documentation xix

Documentation Feedback xx

Obtaining Technical Assistance xx

Cisco.com xx

Technical Assistance Center xxi

Cisco TAC Web Site xxi

Cisco TAC Escalation Center xxii

CHAPTER 1

Overview 1-1

Key Features 1-2

Management Options 1-4

Roaming Client Devices 1-4

Quality of Service Support 1-5

What is QoS? 1-5

Limitations and Restrictions 1-5

Related Documents 1-6

VLAN Support	1-6
What is a VLAN?	1-6
Related Documents	1-9
Incorporating Wireless Devices into VLANs	1-9
A VLAN Example	1-10
Network Configuration Examples	1-12
Root Unit on a Wired LAN	1-12
Repeater Unit that Extends Wireless Range	1-13
Central Unit in an All-Wireless Network	1-14

CHAPTER 2

Using the Management Interfaces	15
Using the Web-Browser Interface	16
Using the Web-Browser Interface for the First Time	16
Using the Management Pages in the Web-Browser Interface	16
Navigating Using the Map Windows	18
Using the Command-Line Interface	19
Preparing to Use a Terminal Emulator	20
Connecting the Serial Cable	20
Setting Up the Terminal Emulator	21
Changing Settings with the CLI	22
Selecting Pages and Settings	23
Applying Changes to the Configuration	23
Navigating the CLI	24
Using SNMP	24
Supported MIBs	25

CHAPTER 3

Configuring the Radio and Basic Settings	3-1
Basic Settings	3-2
Entering Basic Settings	3-2

System Name	3-3
Configuration Server Protocol	3-3
Default IP Address	3-4
Default IP Subnet Mask	3-4
Default Gateway	3-4
Radio Service Set ID (SSID)	3-4
Role in Radio Network	3-5
Radio Network Optimization (Optimize Radio Network For)	3-7
Radio Network Compatibility (Ensure Compatibility With)	3-7
SNMP Admin. Community	3-7
Radio Configuration	3-8
Entering Identity Information	3-8
Settings on the AP Radio Identification Page	3-9
Entering Radio Hardware Information	3-11
Settings on the AP Radio Hardware Page	3-12
Entering Advanced Configuration Information	3-19
Settings on the AP Radio Advanced Page	3-20
Ethernet Configuration	3-28
Entering Identity Information	3-28
Settings on the Ethernet Identification Page	3-29
Entering Ethernet Hardware Information	3-31
Settings on the Ethernet Hardware Page	3-31
Entering Advanced Configuration Information	3-34
Settings on the Ethernet Advanced Page	3-34

CHAPTER 4
Configuring VLANs 4-1

Entering VLAN Information	4-2
Settings on the VLAN Setup page	4-2
VLAN Summary Status Link	4-3
VLAN (802.1Q) Tagging	4-3

802.1Q Encapsulation Mode	4-3
Maximum Number of Enabled VLAN IDs	4-3
Native VLAN ID	4-3
Single VLAN ID which allows Unencrypted packets	4-3
Optionally allow Encrypted packets on the unencrypted VLAN	4-4
VLAN ID	4-4
VLAN Name	4-4
Existing VLANs	4-4
VLAN Security Policy	4-4
Broadcast Domain Segmentation	4-5
Native VLAN Configuration	4-5
Primary and Secondary SSIDs	4-6
RADIUS-Based VLAN Access Control	4-6
Guidelines for Deploying Wireless VLANs	4-8
Criteria for Wireless VLAN Deployment	4-8
A Wireless VLAN Deployment Example	4-9
Using the Configuration Screens	4-10
Obtaining and Recording VLAN ID and Setup Information	4-10
Creating and Configuring VLANs on the Access Point	4-11
Creating the Native VLAN	4-11
Creating the Full- and Part-Time VLANs	4-13
Creating the Guest VLAN	4-14
Creating the Maintenance VLAN	4-14
Creating and Configuring the SSIDs	4-15
Enabling VLAN (802.1Q) Tagging and Identifying the Native VLAN	4-17
Creating an SSID for Infrastructure Devices	4-19
Rules and Guidelines for Wireless VLAN Deployment	4-19

CHAPTER 5**Configuring Filters and Quality of Service 5-1****Filter Setup 5-2****Protocol Filtering 5-2****Creating a Protocol Filter 5-3****Enabling a Protocol Filter 5-5****MAC Address Filtering 5-6****Creating a MAC Address Filter 5-7****QoS Configuration 5-10****Entering Information on the Quality of Service Setup Page 5-10****Settings on the Quality of Service Setup Page 5-11****Generate QBSS Element 5-11****Use Symbol Extensions 5-11****Send IGMP General Query 5-12****Traffic Category 5-12****Applying QoS 5-12****By Station 5-12****By VLAN 5-14****By Filter 5-15****By CoS Value 5-16****By DSCP Value 5-16****A Wireless QoS Deployment Example 5-17****WEP Set on the Wireless Phone 5-19****WEP Not Set on the Wireless Phone 5-19**

CHAPTER 6**Configuring Proxy Mobile IP 6-1****Proxy Mobile IP 6-2****Overview 6-2****Components of a Proxy Mobile IP Network 6-3****How Proxy Mobile IP Works 6-4**

Agent Discovery	6-4
Subnet Map Exchange	6-5
Registration	6-6
Tunneling	6-7
Proxy Mobile IP Security	6-8
The Proxy Mobile IP Setup Page	6-9
General	6-10
Settings on the Proxy Mobile IP General Page	6-10
Authentication Server	6-11
Settings on the Authenticator Configuration Page	6-12
Local SA Bindings	6-13
Settings on the Local SA Bindings Page	6-14
Statistics	6-15
Settings on the Proxy Mobile IP Statistics Page	6-16
View Subnet Map Table	6-18
Settings on the Subnet Map Table Page	6-19
Configuring Proxy Mobile IP	6-19
Before You Begin	6-20
Configuring Proxy Mobile IP on Your Wired LAN	6-20
Configuring the Authoritative Access Point	6-21
Configuring the Access Point on a Home or Foreign Network	6-23

CHAPTER 7

Configuring Other Settings 7-1

Server Setup	7-2
Entering Time Server Settings	7-2
Settings on the Time Server Setup Page	7-3
Simple Network Time Protocol	7-3
Default Time Server	7-3
GMT Offset (hr)	7-3
Use Daylight Savings Time	7-3

Manually Set Date and Time	7-3
Entering Boot Server Settings	7-4
Settings on the Boot Server Setup Page	7-4
Configuration Server Protocol	7-5
Use Previous Configuration Server Settings	7-5
Read .ini File from File Server	7-5
BOOTP Server Timeout (sec)	7-5
DHCP Multiple-Offer Timeout (sec)	7-5
DHCP Requested Lease Duration (min)	7-5
DHCP Minimum Lease Duration (min)	7-6
DHCP Client Identifier Type	7-6
DHCP Client Identifier Value	7-7
DHCP Class Identifier	7-7
Entering Web Server Settings and Setting Up Access Point Help	7-7
Settings on the Web Server Setup Page	7-8
Allow Non-Console Browsing	7-8
HTTP Port	7-8
Default Help Root URL	7-8
Extra Web Page File	7-8
Default Web Root URL	7-9
Entering Name Server Settings	7-9
Settings on the Name Server Setup Page	7-9
Domain Name System	7-10
Default Domain	7-10
Domain Name Servers	7-10
Domain Suffix	7-10
Entering FTP Settings	7-10
Settings on the FTP Setup Page	7-11
File Transfer Protocol	7-11
Default File Server	7-11

FTP Directory	7-11
FTP User Name	7-11
FTP User Password	7-11
Routing Setup	7-11
Entering Routing Settings	7-12
Default Gateway	7-12
New Network Route Settings	7-12
Installed Network Routes List	7-13
Association Table Display Setup	7-13
Association Table Filters Page	7-13
Settings on the Association Table Filters Page	7-14
Stations to Show	7-14
Fields to Show	7-14
Packets To/From Station	7-15
Bytes To/From Station	7-15
Primary Sort	7-15
Secondary Sort	7-15
Association Table Advanced Page	7-16
Settings on the Association Table Advanced Page	7-17
Handle Station Alerts as Severity Level	7-17
Maximum number of bytes stored per Station Alert packet	7-17
Maximum Number of Forwarding Table Entries	7-17
Rogue AP Alert Timeout (minutes)	7-17
Aironet Extended Statistics in MIB (awcTpFdbTable)	7-18
Block ALL Inter-Client Communications (PSPF)	7-18
Default Activity Timeout (seconds) Per Device Class	7-18
Event Notification Setup	7-18
Event Display Setup Page	7-18
Settings on the Event Display Setup Page	7-19
How should time generally be displayed?	7-19

How should Event Elapsed (non-wall-clock) Time be displayed?	7-19
Severity Level at which to display events	7-20
Event Handling Setup Page	7-21
Settings on the Event Handling Setup Page	7-22
Disposition of Events	7-23
Handle Station Events as Severity Level	7-23
Maximum memory reserved for Detailed Event Trace Buffer (bytes)	7-23
Download Detailed Event Trace Buffer	7-23
Clear Alert Statistics	7-23
Purge Trace Buffer	7-23
Event Notifications Setup Page	7-24
Settings on the Event Notifications Setup Page	7-25
Should Notify-Disposition Events generate SNMP Traps?	7-25
SNMP Trap Destination	7-25
SNMP Trap Community	7-25
Should Notify-Disposition Events generate Syslog Messages?	7-25
Should Syslog Messages use the Cisco EMBLEM Format	7-25
Syslog Destination Address	7-26
Syslog Facility Number	7-26
IEEE SNMP Traps Should Generate the Following Notifications	7-26

CHAPTER 8

Security Setup 8-1

Security Overview	8-2
Levels of Security	8-2
Encrypting Radio Signals with WEP	8-3
Additional WEP Security Features	8-3
Network Authentication Types	8-4

Combining MAC-Based, EAP, and Open Authentication	8-8
Protecting the Access Point Configuration with User Manager	8-9
Setting Up WEP	8-9
Using SNMP to Set Up WEP	8-13
Enabling Additional WEP Security Features	8-13
Enabling Message Integrity Check (MIC)	8-14
Enabling Temporal Key Integrity Protocol (TKIP)	8-16
Enabling Broadcast WEP Key Rotation	8-18
Setting Up Open or Shared Key Authentication	8-19
Setting Up EAP Authentication	8-20
Enabling EAP on the Access Point	8-20
Enabling EAP in Cisco Secure ACS	8-25
Setting a Session-Based WEP Key Timeout	8-26
Setting up a Repeater Access Point as a LEAP Client	8-27
Setting Up MAC-Based Authentication	8-29
Enabling MAC-Based Authentication on the Access Point	8-29
Authenticating Client Devices Using MAC Addresses or EAP	8-34
Enabling MAC-Based Authentication in Cisco Secure ACS	8-35
Summary of Settings for Authentication Types	8-37
Setting Up Backup Authentication Servers	8-40
Setting Up Administrator Authorization	8-41
Creating a List of Authorized Management System Users	8-42
Setting up Centralized Administrator Authentication	8-45

CHAPTER 9

Network Management 9-1

Using the Association Table	9-2
Browsing to Network Devices	9-2
Setting the Display Options	9-3

Using Station Pages	9-3
Information on Station Pages	9-4
Performing Pings and Link Tests	9-8
Clearing and Updating Statistics	9-10
Deauthenticating and Disassociating Client Devices	9-10
Using the Network Map Window	9-11
Using Cisco Discovery Protocol	9-12
Settings on the CDP Setup Page	9-13
MIB for CDP	9-13
Assigning Network Ports	9-13
Settings on the Port Assignments Page	9-15
Enabling Wireless Network Accounting	9-15
Settings on the Accounting Setup Page	9-16
Accounting Attributes	9-18

CHAPTER 10
Managing Firmware and Configurations 10-1

Updating Firmware	10-2
Updating with the Browser from a Local Drive	10-2
Full Update of the Firmware Components	10-3
Selective Update of the Firmware Components	10-4
Updating from a File Server	10-5
Full Update of the Firmware Components	10-5
Selective Update of the Firmware Components	10-7
Retrieving Firmware and Web Page Files	10-7
Distributing Firmware	10-9
Distributing a Configuration	10-11
Downloading, Uploading, and Resetting the Configuration	10-12
Downloading the Current Configuration	10-13
Uploading a Configuration	10-14

Uploading from a Local Drive	10-14
Uploading from a File Server	10-15
Resetting the Configuration	10-16
Restarting the Access Point	10-17

CHAPTER 11

Management System Setup 11-1

SNMP Setup	11-2
Settings on the SNMP Setup Page	11-2
Using the Database Query Page	11-3
Settings on the Database Query Page	11-4
Changing Settings with the Database Query Page	11-4
Console and Telnet Setup	11-5
Settings on the Console/Telnet Page	11-5
Using Secure Shell	11-6

CHAPTER 12

Special Configurations 12-1

Setting Up a Repeater Access Point	12-2
Using Hot Standby Mode	12-6

CHAPTER 13

Diagnostics and Troubleshooting 13-1

Using Diagnostic Pages	13-2
Network Diagnostics Page	13-2
Selections on the Network Diagnostics Page	13-3
Carrier Test	13-4
Network Ports Page	13-6
Identifying Information and Status	13-7
Data Received	13-7
Data Transmitted	13-8
Ethernet Port Page	13-9

AP Radio Page	13-12
Event Log Page	13-16
Display Settings	13-16
Log Headings	13-17
Saving the Log	13-17
Event Log Summary Page	13-18
Using Command-Line Diagnostics	13-19
Entering Diagnostic Commands	13-20
Diagnostic Command Results	13-21
:eap_diag1_on	13-21
:eap_diag2_on	13-22
:vxdiag_arpshow	13-22
:vxdiag_checkstack	13-24
:vxdiag_hostshow	13-25
:vxdiag_i	13-26
:vxdiag_ipstatshow	13-27
:vxdiag_memshow	13-28
:vxdiag_muxshow	13-29
:vxdiag_routeshow	13-30
:vxdiag_tcpstatshow	13-31
:vxdiag_udpstatshow	13-32
Tracing Packets	13-32
Reserving Access Point Memory for a Packet Trace Log File	13-32
Tracing Packets for Specific Devices	13-33
Tracing Packets for Ethernet and Radio Ports	13-34
Viewing Packet Trace Data	13-35
Packets Stored in a Log File	13-36
Packets Displayed on the CLI	13-37
Checking the Top Panel Indicators	13-37
Finding an Access Point by Blinking the Top Panel Indicators	13-40

Checking Basic Settings	13-40
SSID	13-40
WEP Keys	13-40
EAP Authentication Requires Matching 802.1X Protocol Drafts	13-41
Resetting to the Default Configuration	13-43
Steps for Firmware Versions 11.07 or Later	13-43
Steps for Firmware Versions 11.06 or Earlier	13-45
Determining the Boot-Block Version	13-45
Reconfiguration Steps for Boot Block Version 1.01 or Earlier	13-46
Reconfiguration Steps for Boot Block Version 1.02 or Later	13-48

APPENDIX A**Menu Tree A-1**

APPENDIX B**Protocol Filter Lists B-1**

APPENDIX C**Channels, Power Levels, and Antenna Gains C-1****Channels C-2****Maximum Power Levels and Antenna Gains C-3**

INDEX INDEX



Preface

The *Cisco Aironet Access Point Software Configuration Guide* describes how to configure Cisco Aironet Access Points using the web-based management system. This manual also briefly describes how to use the console-based management system.

The preface contains the following information:

- Audience and Scope, page xvi
- Organization, page xvi
- Conventions, page xvii
- Related Publications, page xviii
- Obtaining Documentation, page xix
- Obtaining Technical Assistance, page xx

Audience and Scope

This guide is for the network manager responsible for configuring a wireless network. Before using the material in this guide, you should be familiar with some of the concepts and terminology of Ethernet and wireless local area networking.

The scope of this guide is to provide the information you need to change the configuration of an access point, use the access point management system to browse to other devices on a wireless network, and troubleshoot problems with the access point that might arise.

Organization

This guide is organized into the following chapters:

Chapter 1, “Overview,” is a functional overview of the access point management system. It describes the features of the management system and the access point’s role in a wireless network.

Chapter 2, “Using the Management Interfaces,” describes how to use the web-based and console-based management interfaces.

Chapter 3, “Configuring the Radio and Basic Settings,” describes the how to use the web-based management system to configure the access point.

Chapter 4, “Configuring VLANs,” describes VLANs and how to create and configure them.

Chapter 5, “Configuring Filters and Quality of Service,” describes Quality of Service (QoS) and provides information about establishing QoS on an access point.

Chapter 6, “Configuring Proxy Mobile IP,” defines proxy Mobile IP and provides information on configuring this feature on your access point.

Chapter 7, “Configuring Other Settings,” identifies and describes other access point configuration settings such as notifications and server setup.

Chapter 8, “Security Setup,” describes how to set up and enable the access point’s security features.

Chapter 9, “Network Management,” describes how to use the web-based management system to browse to other devices on a wireless network.

Chapter 10, “Managing Firmware and Configurations,” describes how to update the access point’s firmware and use the management system to distribute firmware and configurations to other access points.

Chapter 11, “Management System Setup,” describes methods of managing the access point other than through the access point management system.

Chapter 12, “Special Configurations,” describes how to set up the access point in network roles other than as a root unit on a wired LAN, such as in repeater or Hot Standby mode.

Chapter 13, “Diagnostics and Troubleshooting,” describes how to identify and resolve some of the problems that might arise when you configure an access point running this software release.

Appendix A, “Menu Tree,” provides an overview of the management system’s menu organization.

Appendix B, “Protocol Filter Lists,” lists the protocols you can select for filtering on the management system’s Protocol Filters pages.

Appendix C, “Channels, Power Levels, and Antenna Gains,” lists the channels supported by the world’s regulatory domains.

Conventions

This publication uses the following conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.

Notes and cautions use the following conventions and symbols:



Note

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.



Tip

Means *the following are useful tips*.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Publications

The following documents provide more information about access points and related products:

- *Quick Start Guide: Cisco Aironet Access Points* describes how to attach cables, power on, and assign an IP address and default gateway for the access point.
- *Cisco Aironet Access Point Hardware Installation Guide* describes the access point's hardware features, its physical and performance characteristics, and how to install the access point.
- *Release Notes for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges* describes features and caveats for access points running firmware release 12.x.
- *Cisco Secure Access Control Server for Windows 2000/NT Servers Version 2.6 User Guide* provides complete instructions for using Cisco Secure ACS, including steps for configuring Cisco Secure ACS to support access points.
- *Quick Start Guide: Cisco Aironet Wireless LAN Adapters* describes how to install and configure PC and PCI client adapter cards for use in a wireless LAN.
- *Cisco Aironet Wireless LAN Adapter Installation and Configuration Guide* provides hardware features, physical and performance characteristics, and installation instructions for PC and PCI Card client adapters. It also provides instructions for installing and using the wireless client adapter utilities.
- *Introduction to Mobile IP* is a white paper, available on Cisco.com, that provides an explanation of Mobile IP and how it is used in wired networks.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com>

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

<http://www.cisco.com/go/subscription>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

<http://www.cisco.com/register/>

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.



Overview

Cisco Aironet access points are wireless LAN transceivers that serve as the center point of a stand-alone wireless network or as the connection point between wireless and wired networks. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

The access point uses a browser-based management system, but you can also configure the access point using a terminal emulator, a Telnet session, Secure Shell (SSH), or Simple Network Management Protocol (SNMP).

This chapter provides information on the following topics:

- Key Features, page 1-2
- Management Options, page 1-4
- Roaming Client Devices, page 1-4
- Network Configuration Examples, page 1-12

Key Features

This section describes the key features of the access point firmware. The following are the key features of this firmware version:

- Multiple IEEE 802.11 service set identifiers (SSIDs) allow you to create different levels of network access and to access virtual LANs (VLANs). You can configure up to 16 separate SSIDs to support up to 16 VLANs. Each VLAN can have a different wireless security configuration so that the devices that support the latest Cisco security enhancements can exist alongside legacy devices. This additional access point functionality enables a variety of users having different security levels to access different parts of the network.
- Quality of service (QoS), which allows various devices on the network to communicate more effectively. The access point now supports QoS for wireless Voice over IP (VoIP) telephones and downlink prioritized channel access for streaming audio and video traffic. Filters can also be set to prioritize traffic based on VLAN, VoIP address-based filters, protocol, or port.
- Proxy Mobile IP provides a method for seamless inter-subnet roaming. When you enable proxy Mobile IP on your access points, client devices that roam from one subnet to the next maintain their IP address and session. The access point acts as a Mobile IP proxy for client devices that do not have mobile IP software installed. The access informs the foreign agent router that the client has roamed to another subnet, while the foreign agent directs the home agent to reroute packets to it.
- Centralized administrator authentication uses an AAA server to authenticate users if the user administration feature is enabled on the access point. When a login is attempted, the AAA server verifies the user login and passes back the appropriate privileges for the user or an administrator.
- Better handling of lost Ethernet links causes a number of actions to be executed when an access point loses backbone connectivity:
 - No action—the access point continues to maintain associations with clients and manages traffic between them, but traffic to the backbone is not passed. When the backbone is restored, the access point begins passing traffic to and from the wired network.

- Switch to repeater mode—the access point tries to connect to a root access point using any of the configured SSIDs. If it cannot connect, all clients are disassociated and the access point removes itself from the wireless network until connectivity is restored.
 - Shut the radio off—all clients are disassociated and the access point removes itself from the wireless network until backbone connectivity is restored.
 - Restrict to SSID—the access point allows association using a restricted SSID (for administrator troubleshooting and diagnosis purposes).
- Authentication server management includes two new features in this release:
 - Display of active authentication servers—for each authentication type: 802.1x/LEAP, MAC, or Admin Authentication (if enabled), the active server is identified by a green color.
 - Automatic return to primary authentication server—if the selected RADIUS server (primary) is not reachable after a predetermined period of time-out and retries, the access point uses the next server listed.
- Reporting access points that fail authentication with LEAP provides a passive method of detecting rogue access points in a LEAP enabled network. It is passive because access points do not actively look for or detect a rogue access point in the wireless network. Instead, the access point depends on LEAP enabled clients to report rogue access points.
- Secure Shell (SSH) support for providing a strong user authentication and encryption of management traffic. SSH is a software package that provides a cryptographically secure replacement for or an alternative to Telnet. It provides strong host-to-host and user authentication as well as secure encrypted communications over a non secure network. The feature operates as follows:
 - The SSH server on the access point listens to its TCP port 22 for requests.
 - When a request from a client is received, the access point sends a public key, supported cipher specification details, and supported authentication type (password only) to the client.
 - The client generates a double encrypted session key and sends it to the access point along with the chosen cipher specification.
 - The access point authenticates the client based on a user ID and password when the user manager feature is enabled.

- If authentication is successful, all management traffic between the client and access point is encrypted using the session key.

Management Options

You can use the access point management system through the following interfaces:

- A web-browser interface
- A command-line interface (CLI), Telnet, and SSH
- Simple Network Management Protocol (SNMP)

The access point's management system pages are organized the same way for the web- browser interface and the CLI. The examples in this manual are all taken from the browser interface. Chapter 2, "Using the Management Interfaces," provides a detailed description of each management option.

Roaming Client Devices

If you have more than one access point in your wireless LAN, wireless client devices can roam seamlessly from one access point to another. The roaming functionality is based on signal quality, not proximity. When a client's signal quality drops, it roams to another access point.

Wireless LAN users are sometimes concerned when a client device stays associated to a distant access point instead of roaming to a closer access point. However, if a client's signal to a distant access point remains strong, the client will not roam to a closer access point. If client devices checked constantly for closer access points, the extra radio traffic would slow throughput on the wireless LAN.

Quality of Service Support

The access point now supports Cisco's QoS, primarily in the area of wireless VoIP telephones from Spectralink and Symbol Technologies Corporation. The access point also provides priority classification, prioritized queueing, and prioritized channel access for other downlink IEEE 802.11 traffic such as streaming audio or video traffic.

With this software release, the access point does not include any QoS enhancements in Cisco IEEE 802.11 client software.

What is QoS?

QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies including Ethernet and wireless LANs. In particular, QoS features provide improved and more predictable network service by providing the following services:

- Improving loss characteristics
- Avoiding and managing network congestion
- Prioritizing service to different kinds of network traffic
- Shaping network traffic
- Setting traffic priorities across the network

Limitations and Restrictions

The QoS implementation on the access point has the following limitations and restrictions:

- Provides only prioritized QoS for downlink traffic on IEEE 802.11 links and does not support a general purpose QoS signalling protocol, uniform admission control, guaranteed bandwidth, and other features that are generally associated with parametrized QoS.
- Supports rudimentary admission control mechanisms for Spectralink and Symbol VoIP phones.

- Does not provide a method for prioritizing uplink traffic on IEEE 802.11 links.
- Does not offer 802.1X authentication for Symbol VoIP phones because those phones do not support an 802.1X type such as LEAP or EAP-TLS.
- The DTIM beacon period must be small to support jitter-sensitive streaming multicast audio and video applications.
- Supports IEEE 802.11e EDCF-like channel access prioritization but does not support IEEE 802.11e QoS frame formats.

Related Documents

The following documents provide more detailed information pertaining to QoS design and configuration:

- *Cisco Internetworking Technology Handbook*
- *Cisco IOS Quality of Service Solutions Command Reference, Version 12.2*

These documents are available on Cisco.com.

VLAN Support

Version 12.00T supports VLAN technology by mapping SSIDs to VLANs. With the multiple-SSID capability, the access point can support up to 16 VLAN subnets.

What is a VLAN?

A switched network can be logically segmented into virtual local-area networks (VLANs), on a physical or geographical basis, or by functions, project teams, or applications. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN regardless of their physical connections to the network or the fact that they might be intermingled with devices for other teams. Reconfiguration of VLANs can be done through software rather than physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment; for example, LAN switches that operate bridging protocols between them with a separate group for each VLAN.

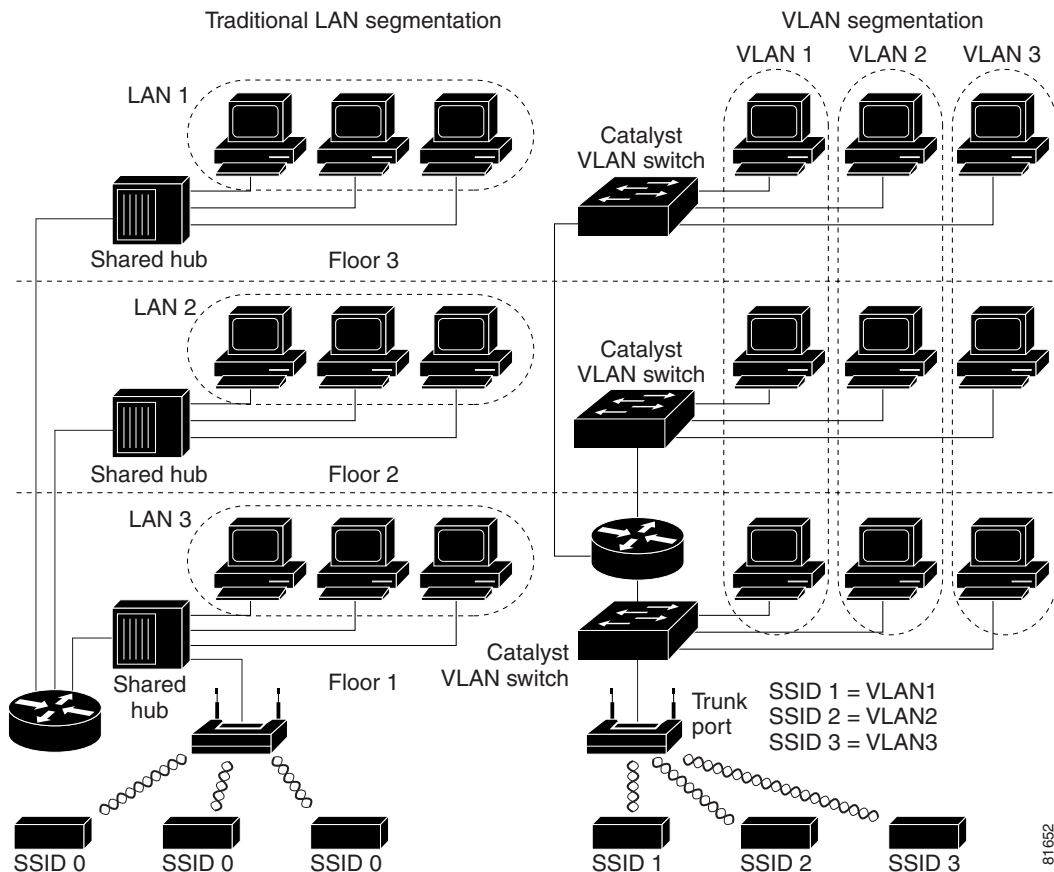
VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic-flow management. None of the switches within the defined group will bridge any frames, not even broadcast frames, between two VLANs. Several key issues must be considered when designing and building switched LAN networks.

- LAN segmentation
- Security
- Broadcast control
- Performance
- Network management
- Communication between VLANs

VLANs are extended into the wireless realm by adding IEEE 802.1Q tag awareness to the access point. Frames destined for wireless LAN clients on different VLANs are transmitted by the access point wirelessly on different SSIDs with different WEP keys. The only clients that can receive and process packets are those with the correct WEP keys. Conversely, packets coming from a client associated with a certain VLAN are 802.1Q tagged before they are forwarded onto the wired network.

Figure 1-1 illustrates the difference between traditional physical LAN segmentation and logical VLAN segmentation with wireless devices connected.

Figure 1-1 LAN Segmentation and VLAN Segmentation with Wireless Components



81652

Related Documents

The following documents provide more detailed information pertaining to VLAN design and configuration:

- *Cisco IOS Switching Services Configuration Guide*
- *Cisco Internetworking Design Guide*
- *Cisco Internetworking Technology Handbook*
- *Cisco Internetworking Troubleshooting Guide*

Incorporating Wireless Devices into VLANs

A WLAN is generally deployed in an enterprise campus or branch office for increased efficiency and flexibility. WLANs are one of the most effective methods to connect to an enterprise network. With version 12.00T, you can configure your wireless devices to operate in a VLAN.

The basic wireless components of a VLAN consist of an access point and a set of clients associated to it using wireless technology. The access point is physically connected through a trunk port to the network switch on which the VLAN is configured. The physical connection to the VLAN switch is through the access point's Ethernet port.

In fundamental terms, the key to configuring an access point to connect to a specific VLAN is by configuring an SSID to map to that VLAN. Because VLANs are identified by a VLAN ID, it follows that if an SSID on an access point is configured to map to a specific VLAN ID, a connection to the VLAN is established. When this connection is made, associated wireless client devices having the same SSID are able to access the VLAN through the access point. The VLAN processes data to and from the clients the same way that it processes data to and from wired connections. The fact that the client is wireless has no impact on the VLAN.

The VLAN feature now enables users to deploy wireless devices with greater efficiency and flexibility. For example, one access point can now handle the specific requirements of multiple users having widely varied network access and permissions. Without VLAN capability, multiple access points, one for each VLAN, would have to be employed to serve classes of users based on the access and permissions they were assigned.

A VLAN Example

The following simplified example shows how wireless devices can be used effectively in a VLAN environment on a college campus. In this example, three levels of access are available through VLANs configured on the physical network:

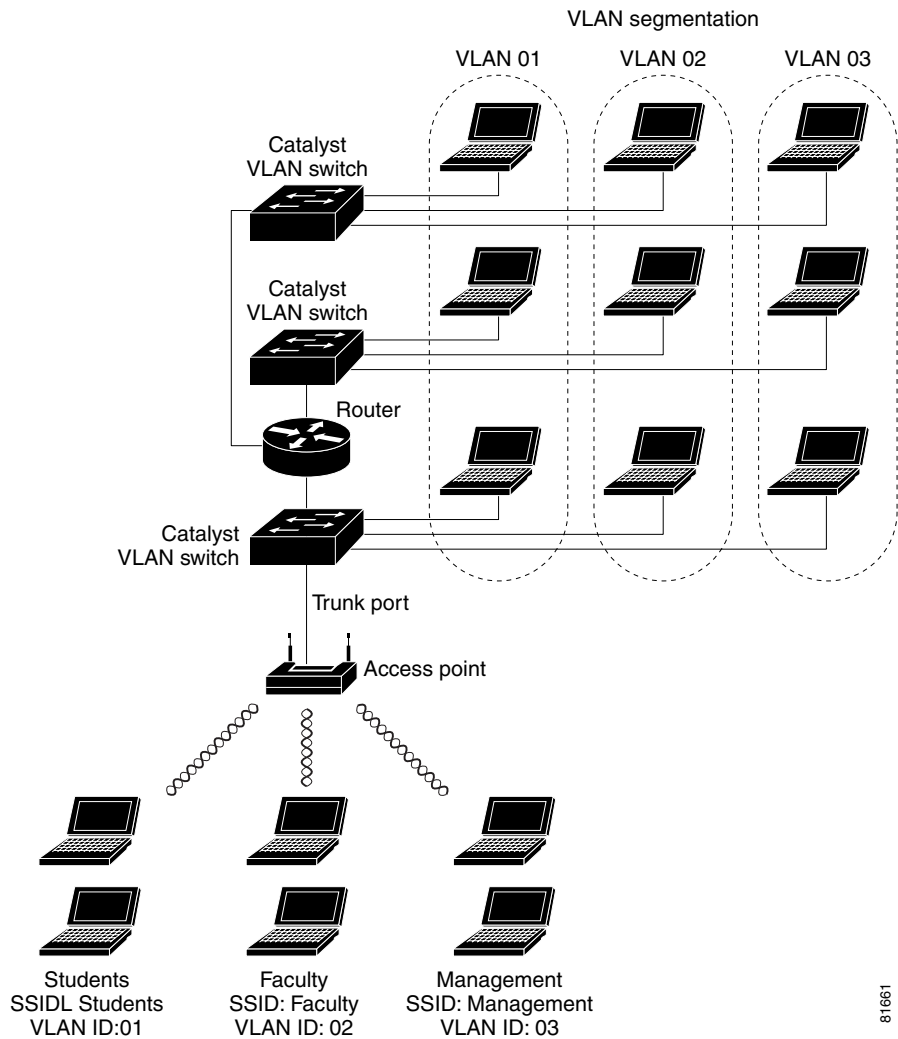
- Student access—Lowest level of access; ability to access school’s Intranet, obtain class schedules and grades, make appointments, and perform other student-related activities
- Faculty access—Medium level of access; ability to access internal files, read to and write from student databases, access the intranet and Internet, and access internal information such as human resources and payroll information
- Management access—Highest level of access; ability to access all internal drives and files, and perform management activities

In this scenario, a minimum of three VLAN connections would be required: one for each level of access discussed above. The access point can handle up to 16 SSIDs; therefore, the following basic design could be employed as shown in Table 1-1.

Table 1-1 Access Level SSID and VLAN Assignment

Level of Access	SSID	VLAN ID
Student	Student	01
Faculty	Faculty	02
Management	Management	03

Using this design, setting up the clients is based on the level of access each user requires. A typical network diagram using this design would look like the one shown in Figure 1-2.

Figure 1-2 VLAN Example

19918

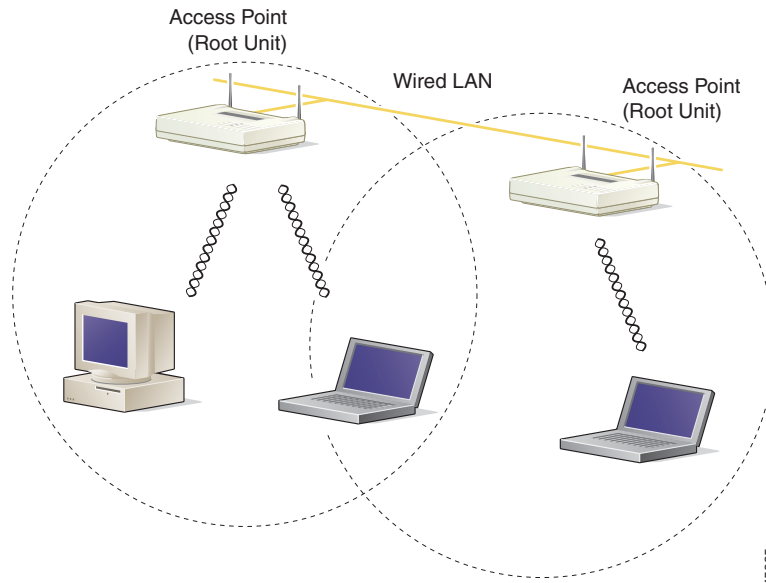
Network Configuration Examples

This section describes the access point's role in three common wireless network configurations. The access point's default configuration is as a root unit connected to a wired LAN or as the central unit in an all-wireless network. The repeater role requires a specific configuration.

Root Unit on a Wired LAN

An access point connected directly to a wired LAN provides a connection point for wireless users. If more than one access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. Figure 1-3 shows access points acting as root units on a wired LAN.

Figure 1-3 Access Points as Root Units on a Wired LAN

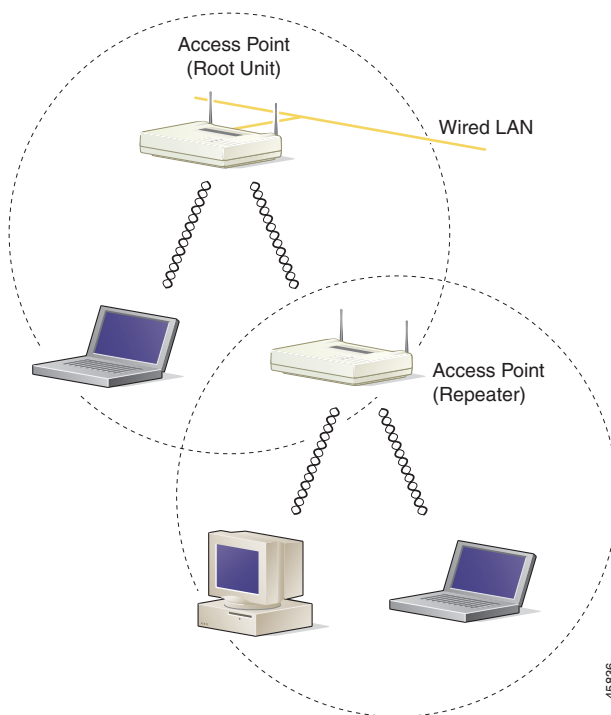


45835

Repeater Unit that Extends Wireless Range

An access point can be configured as a stand-alone repeater to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. Figure 1-4 shows an access point acting as a repeater. Consult the “Setting Up a Repeater Access Point” section on page 12-2 for instructions on setting up an access point as a repeater.

Figure 1-4 Access Point as Repeater

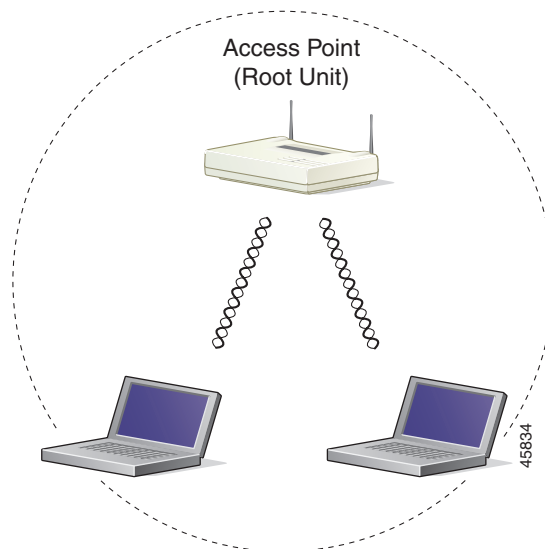


45836

Central Unit in an All-Wireless Network

In an all-wireless network, an access point acts as a stand-alone root unit. The access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. Figure 1-5 shows an access point in an all-wireless network.

Figure 1-5 Access Point as Central Unit in All-Wireless Network





Using the Management Interfaces

This chapter describes the interfaces you can use to configure the access point. You can use a web-browser interface, a command-line interface through a terminal emulator or a Telnet session, or a Simple Network Management Protocol (SNMP) application. The access point's management system web pages are organized the same way for the web browser and command-line interfaces. The examples in this manual show the web-browser interface.

This chapter contains the following sections:

- Using the Web-Browser Interface, page 2-16
- Using the Command-Line Interface, page 2-19
- Using SNMP, page 2-24

Using the Web-Browser Interface

The web-browser interface contains management pages that you use to change access point settings, upgrade and distribute firmware, and monitor and configure other wireless devices on the network.

**Note**

The access point management system is fully compatible with Microsoft Internet Explorer versions 4.0 or later and Netscape Communicator versions 4.0 or later. Earlier versions of these browsers cannot use all features of the management system.

Using the Web-Browser Interface for the First Time

Use the access point's IP address to browse to the management system. See the *Quick Start Guide: Cisco Aironet 350 Series Access Points* for instructions on assigning an IP address to the access point.

Follow these steps to begin using the web-browser interface:

Step 1 Start the browser.

Step 2 Enter the access point's IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer) and press **Enter**.

If the access point has not been configured, the Express Setup page appears. If the access point has been configured, the Summary Status page appears.

Using the Management Pages in the Web-Browser Interface

The system management pages use consistent techniques to present and save configuration information. Navigation buttons appear at the top of the page, and configuration action buttons appear at the bottom. You use the navigation buttons to display other management pages, and you use the configuration action buttons to save or cancel changes to the configuration.

**Note**

It's important to remember that clicking your browser's Back button is the same as clicking **Cancel**: if you make changes on a management page, your changes are not applied when you click **Back**. Changes are only applied when you click **Apply** or **OK**.

Table 2-1 lists the page links and buttons that appear on most management pages.

Table 2-1 Common Buttons on Management Pages

Button/Link	Description
Navigation Links	
Home	Displays the Summary Status page.
Map	Opens the Map window, which contains links to every management page.
Network	Displays the Network Ports page.
Associations	Displays the Association Table page, which provides a list of all devices on the wireless network and links to the devices.
Setup	Displays the Setup page, which contains links to the management pages with configuration settings.
Logs	Displays the Event Log page, which lists system events and their severity levels.
Help	Displays the online help for the current window and the online help table of contents.
Login	Logs you into the access point's management system for access to all pages and features appropriate for your user level.
Configuration Action Buttons	
Apply	Saves changes made on the page and remain on the page.
OK	Saves changes made on the page and return to the previous page.
Cancel	Discards changes to the page and return to the previous page.
Restore Defaults	Returns all settings on the page to their default values.

Navigating Using the Map Windows

The Map window appears when you click **Map** at the top of any management page. You can use the Map window to jump quickly to any system management page, or to a map of your entire wireless network.

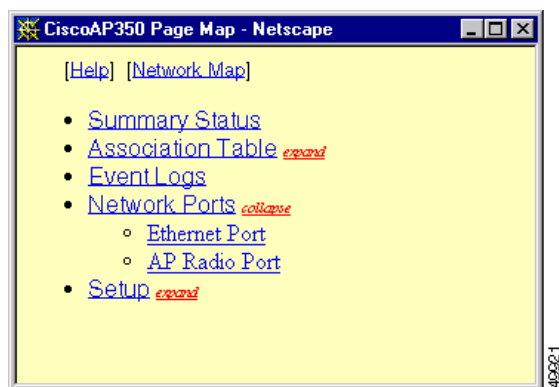


Note

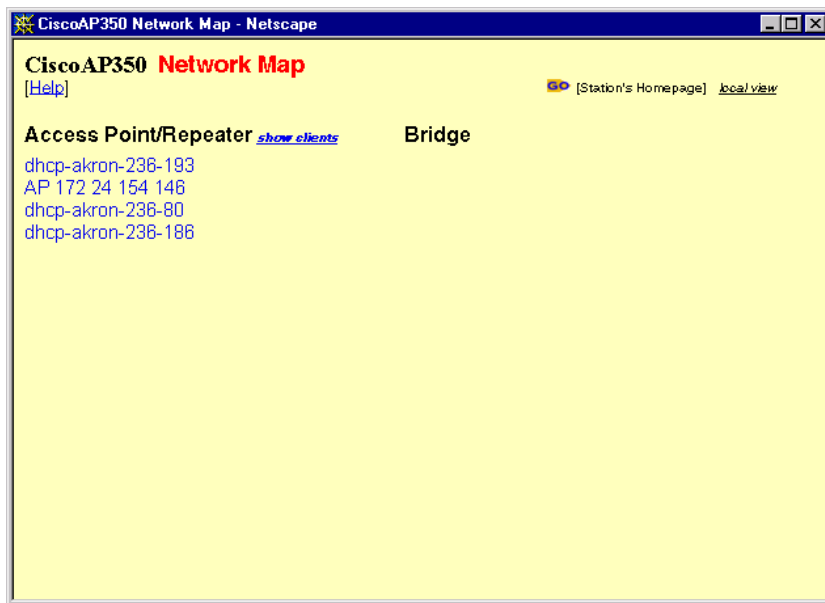
Your Internet browser must have Java enabled to use the map windows.

To display the sub-pages for each main page, click the bullet next to a main page link (Microsoft Internet Explorer), or click **expand** next to a main page link (Netscape Communicator). In Figure 2-1, the sub-pages for the Network Ports page are expanded.

Figure 2-1 Map Window with Network Ports Pages Expanded



The Network Map window appears when you click **Network Map** in the Map window. You use the Network Map window to open a new browser window displaying information for any device on your wireless network. Figure 2-2 shows the Network Map window.

Figure 2-2 The Network Map Window

Click the name of a wireless device to open a new browser window displaying a Station page listing the access point's local information for that device. Click **Go** beside the device name to open a new browser window displaying that device's home page, if available. Some devices, such as PC Card clients, might not have home pages.

Click **show clients** to display all the wireless client devices on your network. The client names appear under the access point or bridge with which they are associated. If clients are displayed, click **hide clients** to display only non-client devices.

Using the Command-Line Interface

You can use a command-line interface (CLI) to configure your access point through a terminal emulation program or a Telnet session instead of through your browser. This section provides instructions for Microsoft's HyperTerminal and for Telnet; other programs are similar.

Preparing to Use a Terminal Emulator

To use a terminal emulator to open the CLI, you need to:

1. Connect a nine-pin, straight-through DB-9 serial cable to the RS-232 serial port on the access point and to the COM port on a computer.
2. Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, Xon/Xoff flow control.

Use the Console/Telnet Setup page to adjust the console and Telnet connection settings. See the “Console and Telnet Setup” section on page 11-5 for details on the Console/Telnet Setup page.

Connecting the Serial Cable

Connect a nine-pin, male-to-female, straight-through serial cable to the COM port on a computer and to the RS-232 serial port on the access point. Figure 2-3 shows the serial port on an access point with a plastic case, and Figure 2-4 shows the location of the serial port on an access point with a metal case.

Figure 2-3 Connecting the Serial Cable on Access Point with Plastic Case

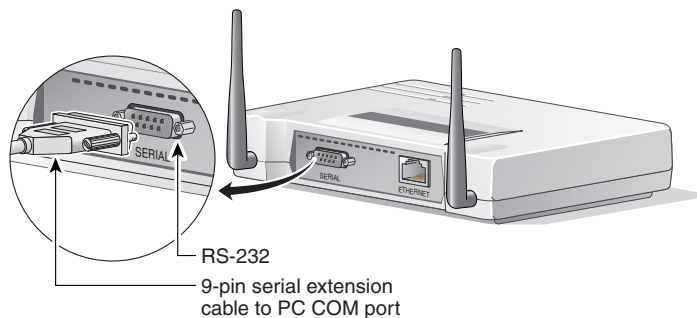
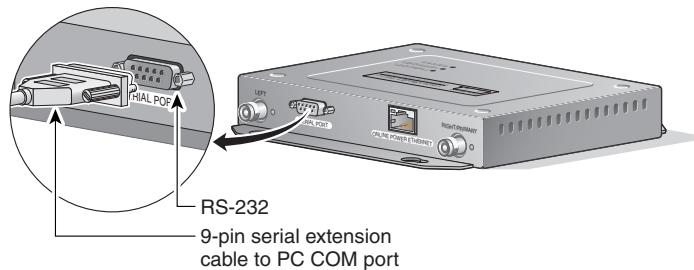


Figure 2-4 Connecting the Serial Cable on Access Point with Metal Case



Setting Up the Terminal Emulator

Follow these steps to set up the terminal emulator:

-
- Step 1** Open a terminal emulator.
- Step 2** Enter these settings for the connection:
- Bits per second (baud rate): 9600
 - Data bits: 8
 - Parity: none
 - Stop bits: 1
 - Flow control: Xon/Xoff
- Step 3** Press = to display the home page of the access point. If the access point has not been configured before, the Express Setup page appears as the home page. If the access point is already configured, the Summary Status page appears as the home page.
-

Changing Settings with the CLI

The CLI pages use consistent techniques to present and save configuration information. Table 2-2 lists the functions that appear on most CLI pages, and Figure 2-5 shows a CLI page example.

Table 2-2 Common Functions on CLI Pages

Function	Description
Press Enter three times	Refreshes the page and cancel changes to settings.
Ctrl-R	Refreshes the page and cancel changes to settings.
=	Returns to the home page without applying changes.
:back	Moves back one page without applying changes.
:bottom	Jumps to the bottom of a long page, such as Event Log. When you are at the bottom of a page, this function becomes <i>:top</i> .
:down	Moves down one page length (24 lines) on a long page, such as Event Log. When you are at the bottom of a long page, this function becomes <i>:up</i> .

Figure 2-5 CLI Page Example

```

CiscoAP350          Console/Telnet Setup          Uptime: 01:32:53

[Baud Rate      ][9600  ]
[Parity         ][None]
[Data Bits      ][8]
[Stop Bits      ][1]
[Flow Control   ][SW Xon/Xoff]
[Terminal Type   ][teletype]
[Columns (64-132)][80  ]
[Lines  (16-50 )][24  ]

[Enable Telnet?][X]

[Apply] [OK]    [Cancel] [Restore Defaults]

[Home] - [Network] - [Associations] - [Setup] - [Logs] - [Help]
[END]

(Auto Apply On) :Back, ^R, =, <ENTER>, or [Link Text]:
  
```

Selecting Pages and Settings


When you type names and settings that appear in brackets you jump to that page or setting. HyperTerminal jumps to the page or setting as soon as it recognizes a unique name, so you only need to type the first few characters in the page or setting name. To jump from the home page to the Setup page, for example, you only need to type **se**.

Applying Changes to the Configuration

The CLI's auto-apply feature is on by default, so changes you make to any page are applied automatically when you move to another management page. To apply changes and stay on the current page, type **apply** and press **Enter**.

Navigating the CLI

The organization of the CLI pages is identical to the web-browser pages. Follow these steps to browse to the CLI pages with Telnet:

-
- Step 1** On your computer's Start menu, select **Programs > Accessories > Telnet**.
If Telnet is not listed in your Accessories menu, select **Start > Run**, type **Telnet** in the entry field, and press **Enter**.
- Step 2** When the Telnet window appears, click **Connect** and select **Remote System**.
-  **Note** In Windows 2000, the Telnet window does not contain pull-down menus. To start the Telnet session in Windows 2000, type **open** followed by the access point's IP address.
-
- Step 3** In the Host Name field, type the access point's IP address and click **Connect**.
-

Using SNMP

You use an SNMP management application to configure the access point with SNMP. Follow these steps to configure the access point with SNMP:

-
- Step 1** Compile the MIB you need to use in your SNMP management application. MIBs supported by the access point are listed in Supported MIBs.
- Step 2** Use a web browser, a Telnet session, or the console interface to open the Express Setup page in the access point management system.
- Step 3** Enter an SNMP community name in the SNMP Admin. Community field and click **OK** or **Apply**.
- Step 4** Follow this link path to reach the SNMP Setup page:
- a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **SNMP** in the Services section of the page.

Use the SNMP Setup page to enter detailed SNMP settings, such as the SNMP trap destination. See the “SNMP Setup” section on page 11-2 for details on the SNMP Setup page.

Supported MIBs

The access point supports the following MIBs:

- AWC-VLAN--MIB.mib
- IEEE802_11Draft6.mib
- AwcVx.mib

These MIBs are bundled in a compressed executable file available on the Software Center at Cisco.com. Follow these steps to download these MIBs:

- Step 1** Browse to <http://www.cisco.com>.
 - Step 2** Click the **Software Center** link. The Software Center home page appears.
 - Step 3** Click **Wireless Software**. The Wireless Software page appears.
 - Step 4** Scroll to the Cisco Aironet Access Point Firmware and Utilities section and click **Cisco Aironet 350 Series**. The Software Download page appears.
 - Step 5** Click the **MIB-AP350vxxxxxx.exe** file for the firmware version your access point is running. The Software License Agreement appears.
 - Step 6** Review the license agreement and then click **Accept**. The Software Download page for the file you selected appears.
 - Step 7** Click **Download: MIB-AP450Vxxxxxx.exe** to begin downloading the file.
 - Step 8** Follow the directions on your screen.
-

You can view and download SNMP and MIB related files on the software center at the following link:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>



Configuring the Radio and Basic Settings

This chapter describes how to use the pages in the access point management system to configure the access point. The main Setup page provides links to all the pages containing access point settings.

This chapter contains the following sections:

- Basic Settings, page 3-2
- Radio Configuration, page 3-8
- Ethernet Configuration, page 3-28

See Chapter 8, “Security Setup” for information on setting up the access point’s security features.

Basic Settings

This section describes the basic settings on the Express Setup page. If you need to set up an access point quickly with a simple configuration, or change or update a basic setting, you can enter all the access point's essential settings for basic operation on the Express Setup page. Figure 3-1 shows the Express Setup page.

Figure 3-1 The Express Setup Page

The screenshot shows the 'Express Setup' page of a Cisco Aironet Access Point. At the top, there are tabs for 'Home', 'Map', and 'Help', and a status indicator 'Uptime: 1 day, 18:11:42'. The main configuration area includes fields for 'System Name' (AP350-41c50a), 'MAC Address' (00:40:96:41:c5:0a), and 'System Serial Number'. Below these are 'Configuration Server Protocol' (set to 'None'), 'Default IP Address' (192.168.141.41), 'Default IP Subnet Mask' (255.255.255.0), and 'Default Gateway' (192.168.141.1). The 'AP Radio' section includes 'Service Set ID (SSID)' (Guest), 'Role in Radio Network' (Root Access Point), 'Optimize Radio Network For' (Throughput selected), and 'Ensure Compatibility With' (2Mb/sec Clients and non-Aironet 802.11). A 'Security Setup' section has an 'SNMP Admin. Community' field (admin1). At the bottom are buttons for 'Apply', 'OK', 'Cancel', and 'Restore Defaults'. A small vertical number '61746' is visible on the right edge of the form.

Follow this link path to reach the Express Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Express Setup**.

Entering Basic Settings

The Express Setup page contains the following configurable settings:

- System Name
- Configuration Server Protocol
- Default IP Address
- Default IP Subnet Mask

- Default Gateway
- Radio Service Set ID (SSID)
- Role in Radio Network
- Radio Network Optimization (Optimize Radio Network For)
- Radio Network Compatibility (Ensure Compatibility With)
- SNMP Admin. Community

System Name

The system name appears in the titles of the management system pages and in the access point's Association Table page. The system name is not an essential setting, but it helps identify the access point on your network.

The access point's Media Access Control (MAC) address appears under the system name. The MAC address is a unique serial number permanently assigned to the access point's Ethernet controller. You cannot change the access point's MAC address.

Configuration Server Protocol

Set the Configuration Server Protocol to match the network's method of IP address assignment. Click the Configuration Server link to jump to the Boot Server Setup page, which contains detailed settings for configuring the access point to work with your network's BOOTP or DHCP servers for automatic assignment of IP addresses.

The Configuration Server Protocol drop-down menu contains the following options:

- None—Your network does not have an automatic system for IP address assignment.
- BOOTP—With Bootstrap Protocol, IP addresses are hard-coded based on MAC addresses.
- DHCP—With Dynamic Host Configuration Protocol, IP addresses are “leased” for predetermined periods of time.

Click **Configuration Server** to access the Boot Server Setup page.

Default IP Address

Use this setting to assign or change the access point's IP address. If DHCP or BOOTP is not enabled for your network, the IP address you enter in this field is the access point's IP address. If DHCP or BOOTP is enabled, this field provides the IP address only if no server responds with an IP address for the access point.

Default IP Subnet Mask

Enter an IP subnet mask to identify the subnetwork so the IP address can be recognized on the LAN. If DHCP or BOOTP is not enabled, this field is the subnet mask. If DHCP or BOOTP is enabled, this field provides the subnet mask only if no server responds to the access point's DHCP or BOOTP request.

Default Gateway

Enter the IP address of your default internet gateway here. The entry 255.255.255.255 indicates no gateway. Clicking the Gateway link takes you to the Routing Setup page, which contains detailed settings for configuring the access point to communicate with the IP network routing system.

Click **Gateway** to access the Routing Setup page where you can configure a new default gateway network route. You can also remove an old routing configuration.

Radio Service Set ID (SSID)

An SSID is a unique identifier that client devices use to associate with the access point or a VLAN supported by the access point. The SSID helps client devices distinguish between multiple wireless networks and VLANs in the same vicinity and provides access to VLANs by wireless client devices. Several access points on a network or sub-network can share an SSID. You can configure up to 16 SSIDs on an access point. An SSID can be any alphanumeric, case-sensitive entry from 2 to 32 characters long.

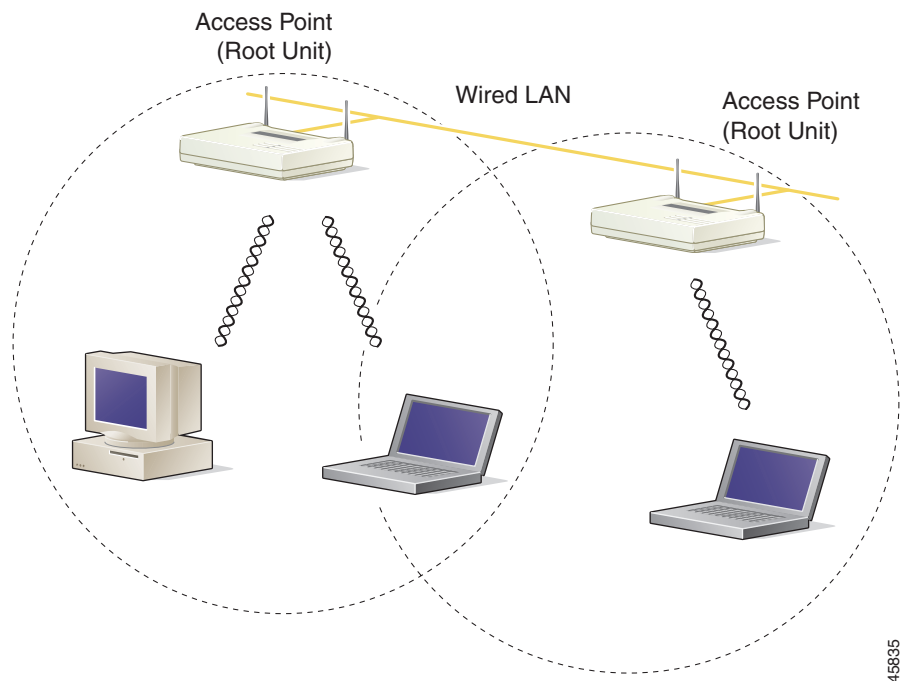
Click **more** to go to the AP Radio Service Sets page where you can create additional SSIDs. From this page you can also edit an existing SSID or remove one from the system.

Role in Radio Network

Use this drop-down menu to select the role of the access point on your network. The menu contains the following options:

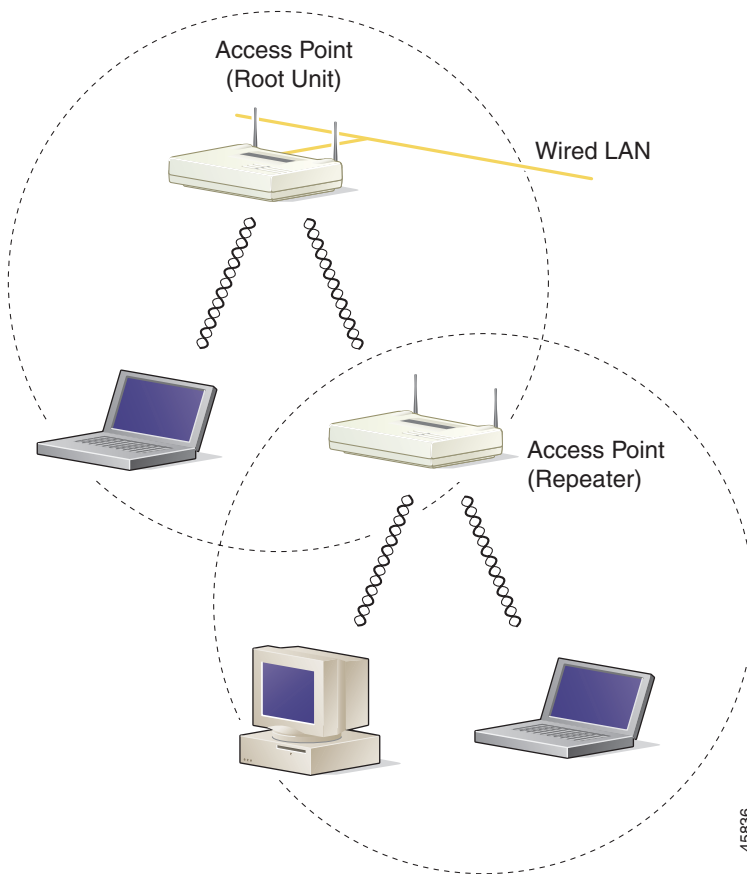
- **Root Access Point**—A wireless LAN transceiver that connects an Ethernet network with wireless client stations. Use this setting if the access point is connected to the wired LAN. Figure 3-2 shows an access point operating as a root unit in a network.

Figure 3-2 Root-Unit Access Points



45835

- **Repeater Access Point**—An access point that transfers data between a client and another access point or repeater. Use this setting for access points not connected to the wired LAN. Figure 3-3 shows an access point operating as a repeater in a network.

Figure 3-3 Repeater Access Point

- **Site Survey Client**—A wireless device that depends on an access point for its connection to the network. Use this setting when performing a site survey for a repeater access point. When you select this setting, clients are not allowed to associate.

Radio Network Optimization (Optimize Radio Network For)

You use this setting to select either pre configured settings for the access point radio or customized settings for the access point radio.

- **Throughput**—Maximizes the data volume handled by the access point but might reduce the access point's range.
- **Range**—Maximizes the access point's range but might reduce throughput.
- **Custom**—The access point uses the settings you enter on the AP Radio Hardware page. Click **Custom** to go to the AP Radio Hardware page.

Radio Network Compatibility (Ensure Compatibility With)

You use this setting to automatically configure the access point to be compatible with other devices on your wireless LAN.

- **2Mb/sec clients**—Select this setting if your network contains Cisco Aironet devices that operate at a maximum speed of 2 Mbps.
- **non-Aironet 802.11**—Select this setting if there are non-Cisco Aironet devices on your wireless LAN.

SNMP Admin. Community

To use Simplified Network Management Protocol (SNMP), enter a community name here. This name automatically appears in the list of users authorized to view and make changes to the access point's management system, and SNMP is enabled.

Click **SNMP** to go to the SNMP Setup page, where you can edit other SNMP settings.

You can define other SNMP communities on the Administrator Authorization pages. See the "Setting Up Administrator Authorization" section on page 8-41 for instructions on using the Administrator Authorization pages.

Radio Configuration

This section describes how to configure the access point's radio. You use the AP Radio pages in the management system to set the radio configuration. The radio pages include:

- **AP Radio Identification**—Contains the basic locating and identity information for the access point Radio port. See the “Entering Identity Information” section on page 3-8 for instructions on using the AP Radio Identification page.
- **AP Radio Hardware**—Contains settings for the access point's SSID, data rates, transmit power, antennas, radio channel, and operating thresholds. See the “Entering Radio Hardware Information” section on page 3-11 for instructions on using the AP Radio Hardware page.
- **AP Radio Advanced**—Contains settings for the operational status of the access point's radio port. You can also use this page to make temporary changes in port status to help with troubleshooting network problems. See the “Entering Advanced Configuration Information” section on page 3-19 for instructions on using the AP Radio Advanced page.
- **AP Radio Port**—Lists key information on the access point's radio port.

Entering Identity Information

You use the AP Radio Identification page to enter basic locating and identity information for the access point radio. Figure 3-4 shows the AP Radio Identification page.

Figure 3-4 The AP Radio Identification Page

Map Help Uptime: 3 days, 17:08:45

Primary Port? ☐ yes ☒ no Adopt Primary Port Identity? ☒ yes ☐ no

MAC Addr.: 00:40:96:40:16:8d

Default IP Address: 10.0.0.2

Default IP Subnet Mask: 255.255.255.0

Current IP Address: 192.168.147.47

Current IP Subnet Mask: 255.255.255.0

Maximum Packet Data Length: 2304

Service Set ID (SSID): SJOLEAP [more...](#)

LEAP User Name:

LEAP Password: *****

Firmware Version: 4.99.68

Boot Block Version: 1.50

Apply OK Cancel Restore Defaults

Follow this link path to reach the AP Radio Identification page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Identification** in the AP Radio row under Network Ports.

Settings on the AP Radio Identification Page

The AP Radio Identification page contains the following settings:

- Primary Port Settings
- Default IP Address
- Default IP Subnet Mask
- Service Set ID (SSID)
- LEAP User Name
- LEAP Password

The page also displays the access point's MAC address, its current IP address, its current IP subnet mask, its maximum packet data length, its firmware version, and its boot block version.

Primary Port Settings

Two options allow you to designate the access point's radio port as the Primary Port and select whether the radio port adopts or assumes the identity of the primary port.

- **Primary Port?**—The primary port determines the access point's MAC and IP addresses. Ordinarily, the access point's primary port is the Ethernet port, which is connected to the wired LAN, so this setting is usually set to **no**. Select **no** to set the Ethernet port as the primary port. Select **yes** to set the radio port as the primary port.
- **Adopt Primary Port Identity?**—Select **yes** to adopt the primary port settings (MAC and IP addresses) for the radio port. Select **no** to use different MAC and IP addresses for the radio port.

Access points acting as root units adopt the primary port settings for the radio port. When you put an access point in standby mode, however, you select **no** for this setting. Some advanced wireless bridge configurations also require different identity settings for the radio port.

Default IP Address

Use this setting to assign an IP address for the radio port that is different from the access point's Ethernet IP address. During normal operation the radio port adopts the identity of the Ethernet port. When you put an access point in standby mode, however, you assign a different IP address to the radio port. Some advanced wireless bridge configurations also require a different IP address for the radio port.

Default IP Subnet Mask

Enter an IP subnet mask to identify the subnetwork so that the IP address can be recognized on the LAN. If DHCP or BOOTP is not enabled, this field is the subnet mask. If DHCP or BOOTP is enabled, this field provides the subnet mask only if no server responds to the access point's request.

The current IP subnet mask displayed under the setting shows the IP subnet mask currently assigned to the access point. This is the same subnet mask as the default subnet mask unless DHCP or BOOTP is enabled. If DHCP or BOOTP is enabled, this is the subnet mask used by the DHCP or BOOTP server.

You can also enter this setting on the Express Setup page.

Service Set ID (SSID)

An SSID is a unique identifier that client devices use to associate with the access point. SSIDs help client devices distinguish between multiple wireless networks in the same vicinity and provide access to VLANs by wireless client devices. Several access points on a network or sub-network can share an SSID. You can configure up to 16 SSIDs on an access point. An SSID can be any alphanumeric, case-sensitive entry from 2 to 32 characters long.

Click **more** to go to the AP Radio Service Sets page where you can create additional SSIDs. From this page you can also edit an existing SSID or remove one from the system.

You can also enter this setting on the Express Setup page.

LEAP User Name

Use this field if the radio is set up as a repeater and authenticates to the network using LEAP. When the radio authenticates using LEAP, the access point sends this user name to the authentication server.

Follow the steps in the “Setting up a Repeater Access Point as a LEAP Client” section on page 8-27 to set up the radio as a LEAP client.

LEAP Password

Use this field if the radio is set up as a repeater and authenticates to the network using LEAP. When the radio authenticates using LEAP, the access point uses this password for authentication.

Follow the steps in the “Setting up a Repeater Access Point as a LEAP Client” section on page 8-27 to set up the radio as a LEAP client.

Entering Radio Hardware Information

You use the AP Radio Hardware page to assign settings related to the access point's radio hardware. Figure 3-5 shows the AP Radio Hardware page.

Figure 3-5 The AP Radio Hardware Page

Map Help Uptime: 3 days, 17:11:59

Service Set ID (SSID): [more...](#)

Allow "Broadcast" SSID to Associate?: ☒ yes ☐ no

Enable "World Mode" multi-domain operation?:

Data Rates (Mb/sec):

1.0 2.0 5.5 11.0

Transmit Power:

Frag. Threshold (256-2338): RTS Threshold (0-2339):

Max. RTS Retries (1-255): Max. Data Retries (1-255):

Beacon Period (19-5000 Kusec): Data Beacon Rate (DTIM):

Default Radio Channel: In Use: 1

Search for less-congested Radio Channel?: [Restrict Searched Channels](#)

Receive Antenna: Transmit Antenna:

IF VLANs are *not* enabled, set Radio Data Encryption through the link below. IF VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through [VLAN Setup](#).

[Radio Data Encryption \(WEP\)](#)

Apply OK Cancel Restore Defaults

Follow this link path to reach the AP Radio Hardware page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Hardware** in the AP Radio row under Network Ports.

Settings on the AP Radio Hardware Page

The AP Radio Hardware page contains the following settings:

- Service Set (SSID)
- Allow Broadcast SSID to Associate?
- Enable World Mode
- Data Rates
- Transmit Power

- Frag. Threshold
- RTS Threshold
- Max. RTS Retries
- Max. Data Retries
- Beacon Period
- Data Beacon Rate (DTIM)
- Default Radio Channel
- Search for Less-Congested Radio Channel
- Restrict Searched Channels
- Receive Antenna and Transmit Antenna

The AP Radio Hardware page also contains links to the AP Radio Data Encryption page and VLAN Setup page. The AP Radio Data Encryption page allows you to enter Wired Equivalent Privacy (WEP) settings if you are not using VLANs. The VLAN Setup page is used to configure WEP settings if you are using VLANs.

Service Set (SSID)

An SSID is a unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity and provides access to VLANs by wireless client devices. Several access points on a network or sub-network can share an SSID. You can configure up to 16 separate SSIDs. The SSID can be any alphanumeric, case-sensitive entry from 2 to 32 characters long.

Click **more** to go to the AP Radio Service Sets page where you can create additional SSIDs. From this page you can also edit an existing SSID or remove one from the system.

You can also enter this setting on the Express Setup and AP Radio Identification pages.

Allow Broadcast SSID to Associate?

You use this setting to choose whether devices that do not specify an SSID (devices that are “broadcasting” in search of an access point to associate with) are allowed to associate with the access point.

- Yes—This is the default setting; it allows devices that do not specify an SSID (devices that are broadcasting in search of an access point to associate with) to associate with the access point.
- No—Devices that do not specify an SSID (devices that are broadcasting in search of an access point to associate with) are not allowed to associate with the access point. With no selected, the SSID used by the client device must match exactly the access point's SSID.

Enable World Mode

When you select **yes** from the world-mode drop-down menu, the access point adds channel carrier set information to its beacon. Client devices with world-mode enabled receive the carrier set information and adjust their settings automatically.

Data Rates

You use the data rate settings to choose the data rates the access point uses for data transmission. The rates are expressed in megabits per second.

The access point always attempts to transmit at the highest data rate set to **Basic**. If there are obstacles or interference, the access point steps down to the highest rate that allows data transmission. For each of four rates (1, 2, 5.5, and 11 megabits per second), a drop-down menu lists three options:

- Basic (default)—Allows transmission at this rate for all packets, both unicast and multicast. At least one of the access point's data rates must be set to Basic.
- Yes—The access point transmits only unicast packets at this rate; multicast packets are sent at one of the data rates set to Basic.
- No—The access point does not transmit data at this rate.

You can use the Data Rate settings to set up an access point to serve client devices operating at specific data rates. For example, to set up the access point for 11 megabits per second (Mbps) service only, select **Basic** for 11 and select **Yes** for the other data rates. Figure 3-6 shows the Data Rates set up for 11-Mbps service only.

Figure 3-6 Data Rate Settings for 11 Mbps Service Only

Data Rates (Mb/sec):

1.0	<input type="button" value="yes"/>	2.0	<input type="button" value="yes"/>	5.5	<input type="button" value="yes"/>	11.0	<input type="button" value="basic"/>
-----	------------------------------------	-----	------------------------------------	-----	------------------------------------	------	--------------------------------------

74126

To set up the access point to serve only client devices operating at 1 and 2 Mbps, select **Basic** for 1 and 2 and set the rest of the data rates to **Yes**. Figure 3-7 shows the Data Rates set up for 1- and 2-Mbps service only.

Figure 3-7 Data Rate Settings for 1- and 2-Mbps Service Only

Data Rates (Mb/sec):

1.0	<input type="button" value="basic"/>	2.0	<input type="button" value="basic"/>	5.5	<input type="button" value="yes"/>	11.0	<input type="button" value="yes"/>
-----	--------------------------------------	-----	--------------------------------------	-----	------------------------------------	------	------------------------------------

74126

The *Optimize Radio Network For* setting on the Express Setup page selects the data rate settings automatically. When you select **Optimize Radio Network For Throughput** on the Express Setup page, all four data rates are set to basic. When you select **Optimize Radio Network For Range** on the Express Setup page, the 1.0 data rate is set to basic, and the other data rates are set to Yes.

Transmit Power

This setting determines the power level of radio transmission.



Note

Government regulations define the highest allowable power level for radio devices. This setting must conform to established standards for the country in which you use the access point.

To reduce interference or to conserve power, select a lower power setting. The settings in the drop-down menu on 350 series access points include 1, 5, 20, 50, and 100 milliwatts. The settings in the drop-down menu on 340 series access points include 1, 5, and 30 milliwatts.



Note

The power settings available on your access point depend on the regulatory domain for which the access point is configured. Your power settings might be different from the settings listed here.

Frag. Threshold

This setting determines the size at which packets are fragmented (sent as several pieces instead of as one block). Enter a setting ranging from 256 to 2338 bytes. Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

RTS Threshold

This setting determines the packet size at which the access point issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the access point and not each other. Enter a setting ranging from 0 to 2339 bytes.

Max. RTS Retries

The maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio. Enter a value from 1 to 128.

Max. Data Retries

The maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.

Beacon Period

The amount of time between beacons in Kilomicroseconds. One Kµsec equals 1,024 microseconds.

Data Beacon Rate (DTIM)

This setting, always a multiple of the beacon period, determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them.

If the beacon period is set at 100, its default setting, and the data beacon rate is set at 2, its default setting, then the access point sends a beacon containing a DTIM every 200 Kµsecs. One Kµsec equals 1,024 microseconds.

Default Radio Channel

The factory setting for Cisco wireless LAN systems is Radio Channel 6 transmitting at 2437 MHz. To overcome an interference problem, other channel settings are available from the drop-down menu of 11 channels ranging from 2412 to 2462 MHz.

Each channel covers 22 MHz. The bandwidth for channels 1, 6, and 11 does not overlap, so you can set up multiple access points in the same vicinity without causing interference.

**Note**

Too many access points in the same vicinity creates radio congestion that can reduce throughput. A careful site survey can determine the best placement of access points for maximum radio coverage and throughput.

Search for Less-Congested Radio Channel

When you select **yes** from the Search for less-congested radio channel drop-down menu, the access point scans for the radio channel that is least busy and selects that channel for use. The access point scans at power-up and when the radio settings are changed.

**Note**

If you need to keep the access point assigned to a specific channel to keep from interfering with other access points, you should leave this setting at **no**.

Restrict Searched Channels

Click **Restrict Searched Channels** to limit the channels that the access point scans when Search for less-congested radio channel is enabled. The AP Radio Restrict Searched Channels page appears when you click Restrict Searched Channels. Figure 3-8 shows the AP Radio Restrict Searched Channels page.

Figure 3-8 AP Radio Restrict Searched Channels Page

Channel Number	Frequency (mHz)	Search?
1	2412	<input checked="" type="checkbox"/>
2	2417	<input checked="" type="checkbox"/>
3	2422	<input checked="" type="checkbox"/>
4	2427	<input checked="" type="checkbox"/>
5	2432	<input checked="" type="checkbox"/>
6	2437	<input checked="" type="checkbox"/>
7	2442	<input checked="" type="checkbox"/>
8	2447	<input checked="" type="checkbox"/>
9	2452	<input checked="" type="checkbox"/>
10	2457	<input checked="" type="checkbox"/>
11	2462	<input checked="" type="checkbox"/>

2001/07/12 10:44:39

Apply OK Cancel Restore Defaults

The page lists all the channels in the access point's regulatory domain. Click the **Search** check boxes beside the channels to include or exclude channels in the scan for less-congested channels. All the channels are included in the scan by default.

Receive Antenna and Transmit Antenna

Drop-down menus for the receive and transmit antennas offer three options:

- **Diversity**—This default setting tells the access point to use the antenna that receives the best signal. If your access point has two fixed (non-removable) antennas, you should use this setting for both receive and transmit.
- **Right**—If your access point has removable antennas and you install a high-gain antenna on the access point's right connector, you should use this setting for both receive and transmit. When you look at the access point's back panel, the right antenna is on the right.
- **Left**—If your access point has removable antennas and you install a high-gain antenna on the access point's left connector, you should use this setting for both receive and transmit. When you look at the access point's back panel, the left antenna is on the left.



Note

The access point receives and transmits using one antenna at a time, so you cannot increase range by installing high-gain antennas on both connectors and pointing one north and one south. When the access point used the north-pointing antenna, it would ignore client devices to the south.

Entering Advanced Configuration Information

Use the AP Radio Advanced page to assign special configuration settings for the access point's radio. Figure 3-9 shows the AP Radio Advanced page.

Figure 3-9 AP Radio Advanced Page

[Map](#)
[Help](#)

Uptime: 3 days, 17:01:17

Requested Status:	Up
Current Status:	Up
Packet Forwarding:	Enabled
Forwarding State:	Forwarding
Default Multicast Address Filter:	Allowed
Maximum Multicast Packets/Second:	0
Radio Cell Role:	Access Point/Root
SSID for use by Infrastructure Stations (such as Repeaters):	0
Disallow Infrastructure Stations on any other SSID:	<input type="radio"/> yes <input checked="" type="radio"/> no
Use Aironet Extensions:	<input checked="" type="radio"/> yes <input type="radio"/> no
Classify Workgroup Bridges as Network Infrastructure:	<input checked="" type="radio"/> yes <input type="radio"/> no
Require use of Radio Firmware 4.99H:	<input checked="" type="radio"/> yes <input type="radio"/> no
Ethernet Encapsulation Transform:	RFC1042

Quality of Service Setup

If VLANs are *not* enabled, set the following three parameters on this page. If VLANs *are* enabled, the following three parameters are set independently for each enabled VLAN through [VLAN Setup](#).

Enhanced MIC verification for WEP:	None
Temporal Key Integrity Protocol:	None
Broadcast WEP Key rotation interval (sec):	0 (0=off)

To configure 802.11 Authentication, EAP, Unicast Address Filters, and the Maximum Number of Associations for this radio's Primary SSID (the default SSID), please use the link below.

[Advanced Primary SSID Setup](#)

Specified Access Point 1:	00:00:00:00:00:00
Specified Access Point 2:	00:00:00:00:00:00
Specified Access Point 3:	00:00:00:00:00:00
Specified Access Point 4:	00:00:00:00:00:00
Radio Modulation:	Standard
Radio Preamble:	Short

[Apply](#)
[OK](#)
[Cancel](#)
[Restore Defaults](#)

Follow this link path to reach the AP Radio Advanced page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Advanced** in the AP Radio row under Network Ports.

Settings on the AP Radio Advanced Page

The AP Radio Advanced page contains the following settings:

- Requested Status
- Current Status
- Packet Forwarding
- Forwarding State
- Default Multicast Address Filters
- Maximum Multicast Packets/Second
- Radio Cell Role
- SSID for use by Infrastructure Stations (such as Repeaters)
- Disallow Infrastructure Stations on any other SSID
- Use Aironet Extensions
- Classify Workgroup Bridges as Network Infrastructure
- Require Use of Radio Firmware x.xx
- Ethernet Encapsulation Transform
- Quality of Service Setup Link
- VLAN Setup Link
- Enhanced MIC verification for WEP
- Temporal Key Integrity Protocol
- Broadcast WEP Key rotation interval (sec)
- Advanced Primary SSID Setup
- Specified Access Points
- Radio Modulation
- Radio Preamble

Requested Status

This setting is useful for troubleshooting problems on your network. Up, the default setting, turns the radio on for normal operation. Down turns the access point's radio off.

Current Status

The Current Status line under the setting displays the current status of the radio port. This field can also display Error, meaning the port is operating but is in an error condition.

Packet Forwarding

This setting is always set to Enabled for normal operation. For troubleshooting, you might want to set packet forwarding to Disabled, which prevents data from moving between the Ethernet and the radio.

Forwarding State

The Forwarding State line under the setting displays the current forwarding state. For normal access point operation, the forwarding state is Forwarding. Four other states are possible:

- Unknown—The state cannot be determined.
- Disabled—Forwarding capabilities are disabled.
- Blocking—The port is blocking transmission. This is the state when no stations are associated.
- Broken—This state reports radio failure.

Default Multicast Address Filters

MAC address filters allow or disallow the forwarding of multicast packets sent to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify. Read the “Creating a MAC Address Filter” section on page 5-7 for complete instructions on setting up MAC address filters.

The drop-down menus for multicast address filters contain two options:

- Allowed—The access point forwards all traffic except packets sent to the MAC addresses listed as disallowed on the Address Filters page.
- Disallowed—The access point discards all traffic except packets sent to the MAC addresses listed as allowed on the Address Filters page.

**Note**

If you plan to discard traffic to all MAC addresses except those you specify (the Disallowed setting), be sure to enter your own MAC address as allowed on the Address Filters page.

Maximum Multicast Packets/Second

Use this setting to control the number of multicast packets that can pass through the radio port each second. If you enter **0**, the access point passes an unlimited number of multicast packets. If you enter a number other than 0, the device passes only that number of multicast packets per second.

Radio Cell Role

Use this drop-down menu to select the function of the access point's radio within its radio coverage area (cell). This setting determines how the access point's radio interacts with other wireless devices. The menu contains the following options:

- Root—A wireless LAN transceiver that connects an Ethernet network with wireless client stations or with another Ethernet network. Use this setting if the access point is connected to the wired LAN.
- Repeater/Non-Root—A wireless LAN transceiver that transfers data between a client and another access point. Use this setting for access points not connected to the wired LAN.
- Client/Non-root—A station with a wireless connection to an access point. Use this setting for diagnostics or site surveys, such as when you need to test the access point by having it communicate with another access point or bridge without accepting associations from client devices.

SSID for use by Infrastructure Stations (such as Repeaters)

Identifies the SSID to be used by repeaters and workgroup bridges to associate to the access point. It is also the SSID used by a non-root bridge to associate to a root bridge. This SSID should be mapped to the native VLAN ID in order to facilitate communications between infrastructure devices and a non-root access point or bridge.

Disallow Infrastructure Stations on any *other* SSID

Prevents repeaters or workgroup bridges from associating to SSIDs other than the infrastructure SSID. The default setting is **No**, so to invoke this condition, you must change the setting to **Yes**.

Use Aironet Extensions

Select **yes** or **no** to use Cisco Aironet 802.11 extensions. This setting must be set to **yes** (the default setting) to enable these features:

- Load balancing—The access point uses Aironet extensions to direct client devices to an access point that provides the best connection to the network based on factors such as number of users, bit error rates, and signal strength.
- Message Integrity Check (MIC)—MIC is an additional WEP security feature that prevents attacks on encrypted packets called *bit-flip* attacks. The MIC, implemented on both the access point and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof.
- Temporal Key Integrity Protocol (TKIP)—TKIP, also known as WEP key hashing, is an additional WEP security feature that defends against an attack on WEP in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key.
- The extensions also improve the access point's ability to understand the capabilities of Cisco Aironet client devices associated with the access point.

Classify Workgroup Bridges as Network Infrastructure

Select **no** to allow more than 20 Cisco Aironet Workgroup Bridges to associate to the access point. The default setting, **yes**, limits the number of workgroup bridges that can associate to the access point to 20 or less.

Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. Treating a workgroup bridge as an infrastructure device means that the access point reliably delivers multicast packets, including Address Resolution Protocol (ARP) packets, to the workgroup bridge.

The performance cost of reliable multicast delivery—duplication of each multicast packet sent to each workgroup bridge—limits the number of infrastructure devices, including workgroup bridges, that can associate to the access point. To increase beyond 20 the number of workgroup bridges that can associate to the access point, the access point must reduce the delivery reliability of multicast packets to workgroup bridges. With reduced reliability, the access point cannot confirm whether multicast packets reach the intended workgroup bridge, so workgroup bridges at the edge of the access point's coverage area might lose IP connectivity. When you treat workgroup bridges as client devices, you increase performance but reduce reliability.

**Note**

This feature is best suited for use with stationary workgroup bridges. Mobile workgroup bridges might encounter spots in the access point's coverage area where they do not receive multicast packets and lose communication with the access point even though they are still associated to it.

A Cisco Aironet Workgroup Bridge provides a wireless LAN connection for up to eight Ethernet-enabled devices. Refer to the “Overview” section on page 1-2 of the *Cisco Aironet Workgroup Bridge Software Configuration Guide* for a description of workgroup bridges.

Require Use of Radio Firmware x.xx

This setting affects the firmware upgrade process when you load new firmware for the access point. Select **yes** to force the radio firmware to be upgraded to a firmware version compatible with the current version of the management system. Select **no** to exempt the current radio firmware from firmware upgrades.

Ethernet Encapsulation Transform

Choose **802.1H** or **RFC1042** to set the Ethernet encapsulation type. Data packets that are not 802.2 packets must be formatted to 802.2 using 802.1H or RFC1042. Cisco Aironet equipment uses 802.1H because it provides optimum interoperability.

- 802.1H—This default setting provides optimum performance for Cisco Aironet wireless products.
- RFC1042—Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment. RFC1042 does not provide the interoperability advantages of 802.1H but is used by other manufacturers of wireless equipment.

Quality of Service Setup Link

Clicking on the Quality of Service (QoS) Setup link accesses the the AP Radio Quality of Service page. Use this page to configure the radio's QoS setup and priorities. Read the "Quality of Service Support" section on page 1-5 for a description of QoS. See the "QoS Configuration" section on page 5-10 to set up QoS.

VLAN Setup Link

Clicking the VLAN Setup link accesses the VLAN Setup page. Use this page to configure, add, edit, and remove VLANs associated with your access point. Read the "VLAN Support" section on page 1-6 for a description of VLANs. Go to the "Creating and Configuring VLANs on the Access Point" section on page 4-11 to set up VLANs.

Enhanced MIC verification for WEP

This setting enables Message Integrity Check (MIC), a security feature that protects your WEP keys by preventing attacks on encrypted packets called *bit-flip* attacks. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC, implemented on both the access point and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof. Select **MMH** from the drop-down menu and click **Apply** to enable MIC.



Note

MIC takes effect only when the Use Aironet Extensions setting on the AP Radio Advanced page is set to **yes** and WEP is enabled and set to full encryption.

**Note**

When you enable MIC, only MIC-capable client devices can communicate with the access point.

Temporal Key Integrity Protocol

This setting enables the temporal key integrity protocol (TKIP, or WEP key hashing), which defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. Select **Cisco** from the drop-down menu and click **Apply** to enable TKIP.

**Note**

To use TKIP, the Use Aironet Extensions setting on the AP Radio Advanced page must be set to **yes** (the default setting).

**Note**

When you enable TKIP, all WEP-enabled client devices associated to the access point must support WEP key hashing. WEP-enabled devices that do not support key hashing cannot communicate with the access point.

Broadcast WEP Key rotation interval (sec)

This option enables broadcast key rotation by setting a key rotation interval. With broadcast, or multicast, WEP key rotation enabled, the access point provides a dynamic broadcast WEP key and changes it at the interval you select. Broadcast key rotation is an excellent alternative to TKIP if your wireless LAN supports wireless client devices that are not Cisco devices or that cannot be upgraded to the latest firmware for Cisco client devices.

To enable broadcast key rotation, enter the rotation interval in seconds in the Broadcast WEP Key rotation interval entry field. If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. To disable broadcast WEP key rotation, enter **0**.

**Note**

When you enable broadcast key rotation, only wireless client devices using LEAP or EAP-TLS authentication can use the access point. Client devices using static WEP (with open, shared key, or EAP-MD5 authentication) cannot use the access point when you enable broadcast key rotation.

Advanced Primary SSID Setup

Go to this link to configure 802.11 authentication, EAP, Unicast address filters, and the maximum number of associations for the radio's primary SSID.

Specified Access Points

You use these fields to set up a chain of repeater access points (access points without an Ethernet connection; see Figure 3-3). Repeater access points function best when they associate with specific access points connected to the wired LAN. You use these fields to specify the access points that provide the most efficient data transmission link for the repeater.

If this access point is a repeater, type the MAC address of one or more root-unit access points with which you want this access point to associate. With MAC addresses in these fields, the repeater access point always tries to associate with the specified access points instead of with other less-efficient access points.

For complete instructions on setting up repeater access points, see the “Setting Up a Repeater Access Point” section on page 12-2.

Radio Modulation

Select **Standard** or **MOK** for the radio modulation the access point uses.

- **Standard**—This default setting is the modulation type specified in IEEE 802.11, the wireless standard published by the Institute of Electrical and Electronics Engineers (IEEE) Standards Association.
- **MOK**—This modulation was used before the IEEE finished the high-speed 802.11 standard and may still be in use in older wireless networks.

Radio Preamble

The radio preamble is a section of data at the head of a packet that contains information the access point and client devices need when sending and receiving packets. The drop-down menu allows you to select a long or short radio preamble:

- Long—A long preamble ensures compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A).
- Short—A short preamble improves throughput performance. Cisco Aironet's Wireless LAN Adapter supports short preambles. Early models of Cisco Aironet's Wireless LAN Adapter (PC4800 and PC4800A) require long preambles.

Ethernet Configuration

This section describes how to configure the access point's Ethernet port. Use the Ethernet pages in the management system to set the Ethernet port configuration. The Ethernet pages include:

- Ethernet Identification—Contains the basic locating and identity information for the Ethernet port.
- Ethernet Hardware—Contains the setting for the access point's Ethernet port connection speed.
- Ethernet Advanced—Contains settings for the operational status of the access point's Ethernet port. You can also use this page to make temporary changes in port status to help with troubleshooting network problems.
- Ethernet Port—Lists key information on the access point's Ethernet port.

Entering Identity Information

You use the Ethernet Identification page to enter basic locating and identity information for the access point's Ethernet port. Figure 3-10 shows the Ethernet Identification page.

Figure 3-10 The Ethernet Identification Page

Map Help Uptime: 3 days, 19:13:23

Primary Port? ☒ yes ☐ no Adopt Primary Port Identity? ☒ yes ☐ no

MAC Addr: 00:40:96:47:89:16

Default IP Address: 192.168.147.47

Default IP Subnet Mask: 255.255.255.0

Current IP Address: 192.168.147.47

Current IP Subnet Mask: 255.255.255.0

Maximum Packet Data Length: 1504

Apply OK Cancel Restore Defaults 01/46

Follow this link path to reach the Ethernet Identification page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Identification** in the Ethernet row under Network Ports.

Settings on the Ethernet Identification Page

The Ethernet Identification page contains the following settings:

- Primary Port Settings
- Default IP Address
- Default IP Subnet Mask

The page also displays the access point's MAC address, the system serial number, its current IP address, its current IP subnet mask, and the maximum packet data length allowed.

Primary Port Settings

Two options allow you to designate the access point's Ethernet port as the Primary Port and select whether the Ethernet port adopts or assumes the identity of the primary port.

- **Primary Port?**—The primary port determines the access point's MAC and IP addresses. Ordinarily, the access point's primary port is the Ethernet port, so this setting is usually set to yes. Select **yes** to set the Ethernet port as the primary port. Select **no** to set the radio port as the primary port.
- **Adopt Primary Port Identity?**—Select **yes** to adopt the primary port settings (MAC and IP addresses) for the Ethernet port. Select **no** to use different MAC and IP addresses for the Ethernet port.

Some advanced bridge configurations require different settings for the Ethernet and radio ports.

Default IP Address

Use this setting to assign or change the access point's IP address. If DHCP or BOOTP is not enabled for your network, the IP address you enter in this field is the access point's IP address. If DHCP or BOOTP is enabled, this field provides the IP address only if no server responds with an IP address for the access point.

The current IP address displayed under the Default IP Address setting shows the IP address currently assigned to the access point. This is the same address as the default IP address unless DHCP or BOOTP is enabled. If DHCP or BOOTP is enabled, this field displays the IP address that has been dynamically assigned to the device for the duration of its session on the network, and it might be different than the default IP address.

You can also enter this setting on the Express Setup and AP Radio Identification pages.

Default IP Subnet Mask

Enter an IP subnet mask to identify the subnetwork so the IP address can be recognized on the LAN. If DHCP or BOOTP is not enabled, this field is the subnet mask. If DHCP or BOOTP is enabled, this field provides the subnet mask only if no server responds to the access point's request.

The current IP subnet mask displayed under the setting shows the IP subnet mask currently assigned to the access point. This is the same subnet mask as the default subnet mask unless DHCP or BOOTP is enabled. If DHCP or BOOTP is enabled, this is the subnet mask used by the server.

You can also enter this setting on the Express Setup and AP Radio Identification pages.

Entering Ethernet Hardware Information

You use the Ethernet Hardware page to select the connector type, connection speed, and duplex setting used by the access point's Ethernet port. Figure 3-11 shows the Ethernet Hardware page.

Figure 3-11 The Ethernet Hardware Page

Map Help 2002/09/30 11:55:17

Speed: Auto

CAM Size: 0

Loss of Backbone Connectivity # of Secs (1-10000): 2

Loss of Backbone Connectivity Action: Switch to repeater mode

Loss of Backbone Connectivity SSID: Native VLAN

This system supports Ethernet-inline power from powered switches. Some models of such switches do not fully support Ethernet speed auto-negotiation. Because of this, selection of "Auto" for Ethernet speed will not take effect until the next **Cold Boot** of this system.

Apply OK Cancel Restore Defaults

Follow this link path to reach the Ethernet Hardware page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Hardware** in the Ethernet row under Network Ports.

Settings on the Ethernet Hardware Page

The Ethernet Hardware page contains the following settings:

- Speed
- Loss of Backbone Connectivity # of Secs (1-10000)
- Loss of Backbone Connectivity Action
- Loss of Backbone Connectivity SSID

The page also displays CAM size and contains a note indicating the the access point supports Ethernet inline power from powered switches.

Speed

The Speed drop-down menu lists five options for the type of connector, connection speed, and duplex setting used by the port. The option you select must match the actual connector type, speed, and duplex settings used to link the port with the wired network.

The default setting, Auto, is best for most networks because the best connection speed and duplex setting are automatically negotiated between the wired LAN and the access point. If you use a setting other than Auto, make sure the hub, switch, or router to which the access point is connected supports your selection.

- Auto—This is the default and the recommended setting. The connection speed and duplex setting are automatically negotiated between the access point and the hub, switch, or router to which the access point is connected.

**Note**

Some switches with inline power do not fully support Ethernet speed auto-negotiation. If your 350 series access point is powered by a switch with inline power, the Auto speed setting is applied only after you reboot the access point.

- 10-Base-T / Half Duplex—Ethernet network connector for 10-Mbps transmission speed over twisted-pair wire and operating in half-duplex mode.
- 10-Base-T / Full Duplex—Ethernet network connector for 10-Mbps transmission speed over twisted-pair wire and operating in full-duplex mode.
- 100-Base-T / Half Duplex—Ethernet network connector for 100-Mbps transmission speed over twisted-pair wire and operating in half-duplex mode.
- 100-Base-T / Full Duplex—Ethernet network connector for 100-Mbps transmission speed over twisted-pair wire and operating in full-duplex mode.

Loss of Backbone Connectivity # of Secs (1-10000)

This setting specifies the amount of time the access point has before taking action when it detects a loss of backbone connectivity (such as a loss of Ethernet link and no active trunks available on its radio). The action the access point takes is specified in the Loss of Backbone Connectivity Action setting, described in the next section.

Loss of Backbone Connectivity Action

This setting determines what action the access point takes when a loss of backbone connectivity occurs after the time specified in the previous setting. The following actions can be taken :

- No action—nothing is done.
- Switch to repeater mode—the access point disassociates all its current clients and becomes a repeater during the period when its backbone connectivity is lost. The access point attempts to communicate with another root access point using the same SSIDs. If it establishes a connection, clients can associate with the root access point through this repeater to maintain connectivity to the backbone LAN. If an appropriate root access point is found, no clients can associate to this access point.
- Shut the radio off—the access point effectively removes itself from the infrastructure by disassociating its current clients and not allowing further associations until backbone connectivity is restored.
- Restrict to SSID—the access point disassociates all its current clients and switches to use the SSID configured in the Loss of Backbone Connectivity: SSID setting. After this action is taken, only a client using the specified SSID can associate with the access point, allowing an administrator to perform failure recovery or diagnostic procedures.

Loss of Backbone Connectivity SSID

This setting specifies the SSID used by the access point if the Loss of Backbone Connectivity Action setting is set as Restrict to SSID and backbone connectivity is lost for longer than the time specified in the Loss of Backbone Connectivity: Number of Seconds setting.

The setting also defines an administrator-only SSID an administrator uses to communicate with the access point for diagnostic and failure-recovery purposes.

If VLANs are active on the access point, the VLAN names are displayed in the Loss of Backbone Connectivity SSID field.

**Note**

When backbone connectivity is restored, the access point restores itself to the settings established during normal operation.

Entering Advanced Configuration Information

You use the Ethernet Advanced page to assign special configuration settings for the access point's Ethernet port. Figure 3-12 shows the Ethernet Advanced page.

Figure 3-12 The Ethernet Advanced Page

Map Help Uptime: 3 days, 19:30:22

Requested Status: Up

Current Status: Up

Packet Forwarding: Enabled

Forwarding State: Forwarding

Default Multicast Address Filter: Allowed

Maximum Multicast Packets/Second: 0

Default Unicast Address Filter: Allowed

Always unblock Ethernet when STP is disabled: ☐ Yes ☒ No

Optimize Ethernet for: Performance

Apply OK Cancel Restore Defaults 61745

Follow this link path to reach the Ethernet Advanced page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Advanced** in the Ethernet row under Network Ports.

Settings on the Ethernet Advanced Page

The Ethernet Advanced page contains the following settings:

- Requested Status
- Packet Forwarding
- Default Unicast and Multicast Address Filter
- Maximum Multicast Packets/Second
- Default Unicast Address Filter
- Optimize Ethernet for

The page also displays the current status of the Ethernet port and its forwarding state. The current status displays either up or down and can also display **Error** if the port is in an error condition.

The forwarding state displays the port's current forwarding state. The state for normal operation is Forwarding. Four other settings are possible:

- **Unknown**—The state cannot be determined
- **Disabled**—Forwarding capabilities are disabled
- **Blocking**—The port is blocking transmission

Broken—This state reports an Ethernet port failure

Requested Status

This setting is useful for troubleshooting problems on your network. Up, the default setting, enables the Ethernet port for normal operation. Down disables the access point's Ethernet port.

The Current Status line under the setting displays the current status of the Ethernet port. This field can also display Error, meaning the port is in an error condition.

Packet Forwarding

This setting is always set to Enabled for normal operation. For troubleshooting, you might want to set packet forwarding to Disabled, which prevents data from moving between the Ethernet and the radio.

The Forwarding State line under the setting displays the current forwarding state. The state for normal operation is Forwarding. Four other settings are possible:

- **Unknown**—The state cannot be determined.
- **Disabled**—Forwarding capabilities are disabled.
- **Blocking**—The port is blocking transmission.
- **Broken**—This state reports an Ethernet port failure.

Default Unicast and Multicast Address Filter

MAC address filters allow or disallow the forwarding of unicast and multicast packets sent to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that

blocks traffic to all MAC addresses except those you specify. Read the “MAC Address Filtering” section on page 5-6 for complete instructions on setting up MAC address filters.

Unicast packets are addressed to just one device on the network. *Multicast* packets are addressed to multiple devices on the network.

The drop-down menus for unicast and multicast address filters contain two options:

- Allowed—The access point forwards all traffic except packets sent to the MAC addresses listed as disallowed on the Address Filters page.
- Disallowed—The access point discards all traffic except packets sent to the MAC addresses listed as allowed on the Address Filters page.

**Note**

For most configurations, you should leave Default Multicast Address Filter set to **Allowed**. If you intend to set it to **Disallowed**, add the broadcast MAC address (ffffffffffff) to the list of allowed addresses on the Address Filters page before changing the setting.

**Note**

If you plan to discard traffic to all MAC addresses except those you specify (the Disallowed setting), be sure to enter your own MAC address as allowed on the Address Filters page.

Maximum Multicast Packets/Second

Use this setting to control the number of multicast packets that can pass through the Ethernet port each second. If you enter **0**, the access point passes an unlimited number of multicast packets. If you enter a number other than 0, the device passes only that number of multicast packets per second.

Default Unicast Address Filter

Use this setting to specify whether the default unicast filter is allowed or disallowed.

Always Unblock Ethernet When STP is Disabled

Use this setting to maintain a bridge link when Spanning Tree Protocol (STP) is disabled. If STP is enabled, select **no**.

Optimize Ethernet for

Use this setting to specify how you want the Ethernet link to perform. You have two choices: performance and statistics collection. Selecting either results in a compromise. However, on a well-designed network, this compromise is virtually unnoticed.



Configuring VLANs

This chapter describes VLANs and provides information about configuring them on an access point. The chapter guides you through the process for configuring a typical example VLAN deployment.

This chapter contains the following sections:

- Entering VLAN Information, page 4-2
- VLAN Security Policy, page 4-4
- RADIUS-Based VLAN Access Control, page 4-6
- Guidelines for Deploying Wireless VLANs, page 4-8
- A Wireless VLAN Deployment Example, page 4-9
- Rules and Guidelines for Wireless VLAN Deployment, page 4-19

Entering VLAN Information

To access the VLAN setup page (see Figure 4-1), click **VLAN** in the Associations section of the Setup page. You can also access the page from the AP Radio Advanced page in the Network Ports section of the Setup page.

Figure 4-1 VLAN Setup Page

The screenshot shows the 'VLAN Setup Page' with a navigation bar at the top containing links: Home, Map, Network, Associations, Setup, Logs, and Help. The 'Setup' link is highlighted. The page title is 'VLAN Summary Status' and the uptime is '4 days, 00:54:09'.

Configuration options include:

- VLAN (802.1Q) Tagging: ☒ Enabled ☐ Disabled
- 802.1Q Encapsulation Mode: Hybrid Trunk
- Maximum Number of enabled VLAN IDs: 16
- Native VLAN ID: 1
- Single VLAN ID which allows Unencrypted packets: 0 (0=all require encryption)
- Optionally allow Encrypted packets on the unencrypted VLAN: ☒ yes ☐ no

Below these options are input fields for 'VLAN ID' and 'VLAN Name', and an 'Add New' button.

The 'Existing VLANs' section shows a list of VLANs:

1	Native VLAN
2	Full-Time
3	Part-Time
4	Guest
5	Maintenance
When VLAN Disabled	

Buttons for 'Edit' and 'Remove' are next to the list. At the bottom are 'Apply', 'OK', 'Cancel', and 'RestoreAll' buttons.

Follow this link path to reach the VLAN Setup page:

1. On the Summary Status page, click **Setup**. The Setup page appears.
2. In the Associations section, click **VLAN**. The VLAN Setup page appears.

Settings on the VLAN Setup page

The VLAN setup page contains the following settings:

- VLAN Summary Status Link
- VLAN (802.1Q) Tagging
- 802.1Q Encapsulation Mode
- Maximum Number of Enabled VLAN IDs
- Native VLAN ID
- Single VLAN ID which allows Unencrypted packets
- Optionally allow Encrypted packets on the unencrypted VLAN
- VLAN ID
- VLAN Name
- Existing VLANs

VLAN Summary Status Link

Clicking this link take you to a page containing a listing of existing VLANs on the access point. The list provides you with configuration information for each VLAN. Figure 4-2 shows a typical VLAN Summary Status page.

Figure 4-2 VLAN Summary Status Page

Home	Map	Network	Associations	Setup	Logs	Help	2002/10/29 14:34:14		
802.1Q Encapsulation Mode: Hybrid Trunk							<u>VLAN Detailed Setup</u>		
ID	Name	Enabled?	Def. Pri.	Def. Pol. Grp.	MIC	TKIP	Key Rotate	Alert?	Encryption
<u>1</u> (N)	Native VLAN	yes	best effort	[0]	none	Cisco	0	no	full
<u>2</u>		no	best effort	[0]	none	none	0	no	optional
<u>3</u>	Part-Time	yes	best effort	[0]	none	Cisco	0	no	full
<u>4</u>	Guest	yes	best effort	[0]	none	none	0	no	optional
<u>5</u>	Maintenance	yes	best effort	[0]	none	none	0	no	full
Done									66167

VLAN (802.1Q) Tagging

Determines whether the IEEE 802.1Q protocol is used to tag VLAN packets. IEEE 802.1Q protocol is used to connect multiple switches and routers and for defining VLAN topologies. This setting is user configurable.

802.1Q Encapsulation Mode

A status setting that indicates whether or not IEEE 802.1Q tagging is in use. When VLANs are successfully configured on the access point, the setting displays “**Hybrid Trunk.**” Otherwise, the setting displays “**Disabled.**” You cannot directly configure this setting; it changes after you successfully create and configure a VLAN on the access point.

Maximum Number of Enabled VLAN IDs

A status setting that provides the maximum number of VLANs that can reside on the access point. This setting is for information only and is not configurable.

Native VLAN ID

Specifies the identification number of the access point’s native VLAN. This configurable setting must agree with the native VLAN ID setting on the switch.

Single VLAN ID which allows Unencrypted packets

Identifies the number of the VLAN on which unencrypted packets can pass between the access point and the switch. This setting is configurable.

Optionally allow Encrypted packets on the unencrypted VLAN

Determines whether the access point passes encrypted packets on an unencrypted VLAN. This setting permits a client device to associate to the access point allowing both WEP and non-WEP associations.

VLAN ID

A unique number that identifies a VLAN. This number must match VLANs set on the switch. The setting is configured by the user.

VLAN Name

A unique name for a VLAN configured on the access point. This setting is configured by the user. The VLAN name is for information only and is not used by the switch or access point as a parameter for determining the destination of data.

Existing VLANs

A list of successfully configured VLANs on the access point. As the user configures VLANs, they appear in this list by ID number and name. From this list, you can edit or remove a VLAN.

VLAN Security Policy

You can define a security policy for each VLAN on the access point. This enables you to define the appropriate restrictions for each VLAN you configure. The following parameters can be configured on the wireless VLAN:

- SSID Name—a unique name for each wireless VLAN
- Default VLAN ID—VLAN ID mapping on the wired side
- Authentication types—Open, Shared, and Network-EAP
- MAC authentication—Under Open, Shared, and Network-EAP
- EAP authentication—Under Open, Shared, and Network-EAP
- Maximum number of associations—ability to limit maximum number of wireless clients per SSID

The following parameters can be configured on the wired VLAN:

- Encryption key—the key used for broadcast or multicast segmentation per VLAN. This key is also used for static WEP clients for both unicast and multicast traffic
- Enhanced MIC verification for WEP—ability to enable MIC per VLAN
- Temporal Key Integrity Protocol (TKIP)—ability to enable per packet key hashing for each VLAN
- WEP key rotation interval—ability to enable WEP key rotation for each VLAN but supported only for wireless VLANs with IEEE 802.1x protocols enabled (such as LEAP, EAP-TLS, PEAP, etc.)
- Default Policy Group—ability to apply a policy group (set of Layer 2, 3, and 4 filters) for each VLAN. Each filter within a policy group can be configured to allow or deny a certain type of traffic
- Default Priority—ability to apply default CoS for each VLAN

**Note**

With an encryption key configured, the VLAN supports standardized WEP. However, TKIP, MIC, and broadcast key rotation features can optionally be configured as noted above.

Table 4-1 lists the SSID and VLAN ID configuration parameters.

Table 4-1 /SSID and VLAN ID Configuration Parameters

Parameter	SSID Parameter	VLAN ID Parameter
Authentication types	x	x
Maximum number of associations	x	
Encryption key (broadcast key)		x
TKIP/MIC		x
WEP rotation interval		x
Policy group		x
Default Priority (CoS mapping)		

Broadcast Domain Segmentation

All Layer 2 broadcast and multicast messages are propagated over the air so that each WLAN client receives broadcast and multicast traffic belonging to different VLANs. A wired client receives Layer 2 broadcast and multicast traffic only for its own VLAN. Therefore, a unique broadcast/multicast encryption key is used to segment the Layer 2 broadcast domains on the wireless LAN. The unique encryption key must be configured during initial VLAN setup. If broadcast key rotation is enabled, this encryption key is generated dynamically and delivered to WLAN clients in IEEE 802.1x messages.

The requirement to segment broadcast domains on the wireless side restricts the use of unencrypted VLAN per ESS. A maximum of one VLAN can be unencrypted per WLAN ESS. The behavior of a WLAN client on an encrypted VLAN should be to discard unencrypted Layer 2 broadcast or multicast traffic.

Native VLAN Configuration

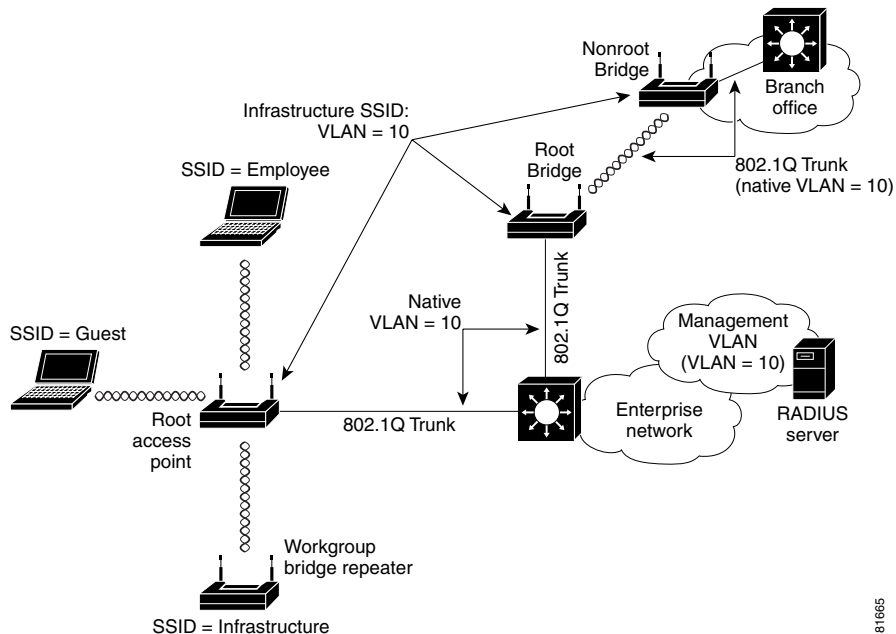
The native VLAN setting on the access point must match the native VLAN of the wired trunk. Also, the access point receives and communicates using the Inter-Access Point Protocol (IAPP) with other access points in the same wireless LAN ESS using the native VLAN. Therefore, it is a requirement that all access points in an ESS use the same native VLAN ID and that all Telnet and http management traffic be routed to the access point on the native VLAN. Cisco recommends that you map the native VLAN of the access point to the management VLAN of the network and do not route the native VLAN of the access point with non-native VLANs.

You may or may not wish to map the native VLAN of the access point to an SSID (for example, to the wireless ESS). Scenarios where the native VLAN must be mapped to an SSID are as follows:

- An associated workgroup bridge to be treated as an infrastructure device
- For a root bridge to connect to a nonroot bridge

In these scenarios, Cisco recommends that you configure an infrastructure SSID for each access point. Figure 4-3 illustrates combined deployment of infrastructure devices along with noninfrastructure devices in an enterprise LAN. As the figure shows, the native VLAN of the access point is mapped to the infrastructure SSID. WEP encryption along with TKIP (at least per packet key hashing) should be turned on for the infrastructure SSID. Cisco also recommends that you configure a secondary SSID as the infrastructure SSID. The concepts of primary and secondary SSIDs are explained in the next section.

Figure 4-3 Deployment of Infrastructure and Noninfrastructure Devices



Primary and Secondary SSIDs

When multiple wireless VLANs are enabled on an access point or bridge, multiple SSIDs are created. Each SSID maps to a default VLAN ID on the wireless side. IEEE 802.11 specifications require that only one SSID be broadcast in the beacons, so you must define a primary SSID to be broadcast in the IEEE 802.11 beacon management frames. All other SSIDs are secondary SSIDs and are not broadcast in the beacon management frames.

If a client or infrastructure device (such as a workgroup bridge) sends a probe request with a secondary SSID, the access point or bridge responds with a probe response with a secondary SSID.

You can map the primary SSID to the VLAN ID on the wired infrastructure in different ways. For example, in an enterprise rollout scenario, the primary SSID could be mapped to the unencrypted VLAN on the wired side to provide guest VLAN access.

RADIUS-Based VLAN Access Control

You may want to impose RADIUS-based VLAN access control. For example, if the WLAN setup is such that all VLANs use IEEE 802.1x and similar encryption mechanisms for WLAN user access, the user can hop from one VLAN to another by changing the SSID and successfully authenticating to the access point. However, this process may not be ideal if the wireless user is to be confined to a particular VLAN.

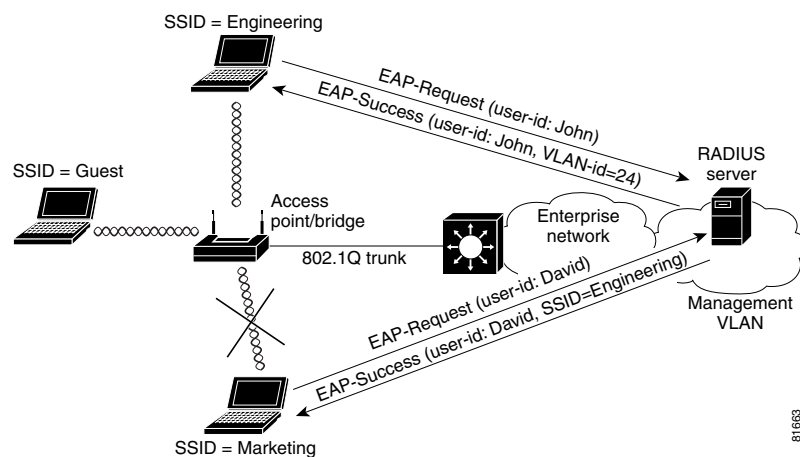
There are two ways to implement RADIUS-based VLAN access control on the access point:

1. **RADIUS-based VLAN assignment**—upon successful IEEE 802.1x authentication, the RADIUS server assigns the user to a particular VLAN ID on the wired side. Regardless of which SSID is used for WLAN access, the user is always assigned to a particular VLAN ID.
2. **RADIUS-based SSID access control**—Upon successful IEEE 802.1x authentication, the RADIUS server passes back the allowed SSID list and the user is allowed to associate to the WLAN. Otherwise, the user is disassociated from the access point or bridge.

Figure 4-4 illustrates both RADIUS-based VLAN access control methods. In the figure, both Engineering and Marketing VLANs are configured to allow only IEEE 802.1x authentication (LEAP, EAP-TLS, PEAP, etc.). When user John uses the Engineering SSID to access the WLAN, the RADIUS server maps John to VLAN ID 24, which may or may not be the default VLAN ID mapping for the Engineering SSID. Using this method, a user can be mapped to a fixed wired VLAN throughout an enterprise network.

Figure 4-4 also shows an example for RADIUS-based SSID access control. In the figure, David uses the Marketing SSID to access the WLAN however, the permitted SSID list sent back by the RADIUS server allows David to access only the Engineering SSID and the access point disassociates him from the WLAN. Using RADIUS-based SSID access, a user can be given access to one or multiple SSIDs throughout the enterprise network.

Figure 4-4 RADIUS-Based VLAN Access Control



RADIUS user attributes used for VLAN ID assignment are:

- IETF 64 (Tunnel Type)—Set this to VLAN
- IETF 65 (Tunnel Medium Type)—Set this to 802
- IETF 81 (Tunnel Private Group ID)—Set this to VLAN ID

The Cisco IOS/PIX/RADIUS Attribute (009\001 cisco-av-pair) user attribute is used for SSID control. For example, this attribute allows a user to access the WLAN using the Engineering and Marketing SSIDs only.

Guidelines for Deploying Wireless VLANs

You should evaluate the need for deploying wireless VLANs in their own environment. Cisco recommends that you review the VLAN deployment rules and policies before considering wireless VLAN deployment and that you use similar policies to extend wired VLANs to the wireless LAN. This section details criteria for wireless VLAN deployment, a summary of rules for wireless LAN (WLAN) VLAN deployment, and best practices to use on the wired infrastructure side when you deploy wireless VLANs.

Criteria for Wireless VLAN Deployment

Criteria for wireless VLAN deployment are likely to be different for each scenario. The following are the most likely criteria:

- Common resources being used by the WLAN:
 - Wired network resources, such as servers, commonly accessed by wireless users
 - QoS level needed by each application (default CoS, voice CoS, etc.)
- Common devices used to access the WLAN, such as the following:
 - Security mechanisms (static WEP, MAC authentication and EAP authentication supported by each device type)
 - Wired network resources, such as servers, commonly accessed by WLAN device groups
 - QoS level needed by each device group
- Revisions to the existing wired VLAN deployment:
 - Existing policies for VLAN access
 - Localized wired VLANs or flat Layer 2 switched network policies
 - Other affected policies

You should consider the following implementation criteria before deploying wireless VLANs:

- Use policy groups (a set of filters) to map wired policies to the wireless side.
- Use IEEE 802.1x to control user access to VLANs by using either RADIUS-based VLAN assignment or RADIUS-based SSID access control.
- Use separate VLANs to implement different classes of service.
- Adhere to any other criteria specific to your organization's network infrastructure.

Based on these criteria, you could choose to deploy wireless VLANs using the following strategies:

- **Segmentation by user groups**—you can segment your WLAN user community and enforce a different security policy for each user group. For example, you could create three wired and wireless VLANs in an enterprise environment for full- and part-time employees, as well as providing guest access.
- **Segmentation by device types**—You can segment your WLAN to enable different devices with different security levels to access the network. For example, you have hand-held devices that support only 40- or 128-bit static WEP coexisting with other devices using IEEE 802.1x with dynamic WEP in the same ESS. Each of these devices would be isolated into separate VLANs.

A Wireless VLAN Deployment Example

This section outlines a typical use of wireless VLANs. For the example, assume your company, XYZ, determines the need for wireless LANs in its network. Following the guidelines in the previous sections, your findings are as follows:

- Five different groups are present at Company XYZ: full-time employees, part-time employees, contract employees, guests, and maintenance workers.
- Full-time and contract employees use company-supplied PCs to access the wireless network. The PCs are capable of supporting IEEE 802.1x authentication methods to access the wireless LAN.
- Full-time employees need full access to the wired network resources. The IT department has implemented application level privileges for each user (using Microsoft NT or 2000 AD mechanisms).
- Part-time and contract employees are not allowed access to certain wired resources (such as HR or data storage servers). The IT department has implemented application level privileges for part time employees (using Microsoft NT or 2000 AD mechanisms).
- Guest users want access to the Internet and are likely to launch a VPN tunnel back to their own company headquarters.
- Maintenance workers use specialized hand-held devices to access information specific to maintenance issues (such as trouble tickets). They access the information from a server in an Application Servers VLAN. The handhelds only support static 40- or 128-bit WEP.
- Existing wired VLANs are localized per building and use Layer-3 policies to prevent users from accessing critical applications.

Using the information above, you could deploy wireless VLANs by creating four wireless VLANs as follows:

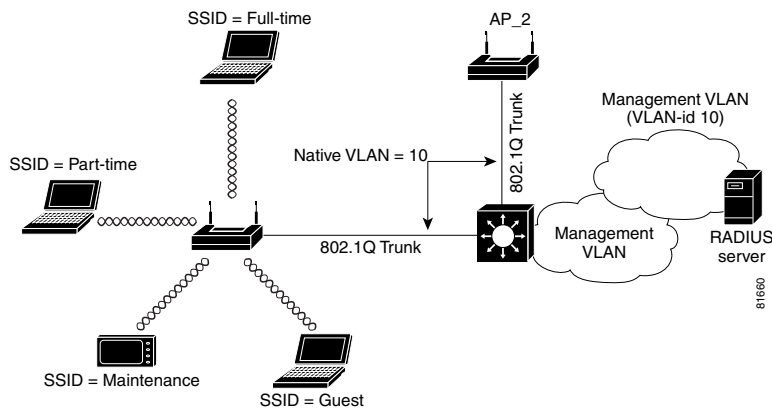
- A *full-time* VLAN and a *part-time* VLAN using IEEE 802.1x with dynamic WEP and TKIP features for WLAN access. User login is tied to the RADIUS server with a Microsoft back-end user database. This configuration enables the possibility of single sign-on for WLAN users.
- RADIUS-based SSID access control for both full-time and part-time employee WLAN access. Cisco recommends this approach to prevent part-time employees from VLAN hopping, such as trying to access the WLAN using the full-time VLAN.

**Note**

In this deployment scenario, VLANs are localized per building, enabling users to access the WLAN from anywhere within the campus. Cisco recommends using SSID access control rather than using fixed VLAN ID assignment.

- A *guest* VLAN uses the primary SSID with open or no WEP access. Policies are enforced on the wired network side to force all guest VLAN access to an Internet gateway and denies access into the XYZ corporate network.
- A *maintenance* VLAN uses open with WEP plus MAC authentication. Policies are enforced on the wired network side to allow access only to the maintenance server on the application server's VLAN.

Figure 4-5 shows the wireless VLAN deployment scenario described above.

Figure 4-5 Wireless VLAN Deployment Example

Using the Configuration Screens

Using the example outlined above, this section describes how to use the configuration screens to configure VLANs on your access point.

To create and enable VLANs on your access point you must complete the following procedures:

1. Obtain and record the VLAN ID and setup information for the switch to which your access point will communicate.
2. Create and configure the VLANs on your access point.
3. Create and configure the SSIDs to which the VLANs will associate.
4. Enable VLAN (802.1Q) tagging.
5. Identify the native VLAN.

Obtaining and Recording VLAN ID and Setup Information

See your organization's network administrator to obtain the information you need to create VLANs on your access point. For this example, Table 4-2 lists the information required to configure the VLANs on the access point.

Table 4-2 Configuration for Example VLAN Deployment

SSID	VLAN ID	Security Policy
Native VLAN	1	IEEE 802.1x with Dynamic WEP + TKIP/MIC
Full-time	2	IEEE 802.1x with Dynamic WEP + TKIP/MIC
Part-time	3	IEEE 802.1x with Dynamic WEP + TKIP/MIC
Guest	5	Open with no WEP
Maintenance	4	Open with WEP + MAC authentication

Creating and Configuring VLANs on the Access Point

For this example, you will create 5 VLANs using the information in Table 3-2.



Note

To avoid error messages in the event log, do not enable the VLANs until you have finished creating them and associated SSIDs to them.

Creating the Native VLAN

You must create and identify a native VLAN before the access point can connect to the trunk and communicate with the switch. Follow these steps to create the native VLAN.

- Step 1** Use your web browser to browse to the access point's summary status page.
- Step 2** Click **Setup**. The Setup page appears.
- Step 3** In the Associations section, click **VLAN**. The VLAN Setup page appears (Figure 4-6).

Figure 4-6 VLAN Setup Page

Home Map Network Associations Setup Logs Help Uptime: 05:50:24

VLAN Summary Status

VLAN (802.1Q) Tagging: ☐ Enabled ☒ Disabled

802.1Q Encapsulation Mode: --Disabled--

Maximum Number of enabled VLAN IDs: 16

Native VLAN ID:

Single VLAN ID which allows **Unencrypted** packets: (0=all require encryption)

Optionally allow **Encrypted** packets on the unencrypted VLAN: ☒ yes ☐ no

VLAN ID: VLAN Name:

Existing VLANs:

VLAN ID	VLAN Name
1	Native VLAN

86507

- Step 4** Enter 1 in the Default VLAN ID field.
- Step 5** Enter Native VLAN in the VLAN Name field.
- Step 6** Click **Add New**. The VLAN ID #1 Setup Page appears (Figure 4-7).

Figure 4-7 VLAN ID #1 Setup Page

Map Help Uptime: 6 days, 00:35:02

VLAN Name: Native VLAN

VLAN Enable: ☒ Enabled ☐ Disabled

Default Priority: default

Default Policy Group: [0] None

Enhanced MIC verification for WEP: None

Temporal Key Integrity Protocol: None

WEP Key Rotation Interval: 0 (0=off)

Alert?: ☐ yes ☒ no

	Encryption Key	Key Size
WEP Key 1:	12345678901234567890123456	128 bit
WEP Key 2:		not set
WEP Key 3:		not set
WEP Key 4:		not set

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
 Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).

Apply OK Cancel Restore Defaults

Step 7 Make the following entries on this page:

- VLAN Name: Native VLAN (should be displayed)
- VLAN Enable: Enable
- Default Priority: default
- Default Policy Group: None
- Enhanced MIC verification for WEP: None
- Temporal Key Integrity Protocol: Cisco
- WEP Key 1: Enter 26 hexadecimal characters.
- Key Size: 128 bit


Step 8 Click **OK** to save your settings and return to the VLAN Setup screen.

Creating the Full- and Part-Time VLANs

The full- and part-time VLANs are essentially the same except for their names and SSIDs. Follow these steps to create these VLANs.

-
- Step 1** On the VLAN Setup page, make the following changes:
- a. VLAN (802.1Q) Tagging: Disabled
 - b. Native VLAN ID: 0
 - c. Single VLAN which allows Unencrypted packets: 0
 - d. Optionally allow Encrypted packets on the unencrypted VLAN: yes
 - e. VLAN ID: 2
 - f. VLAN Name: Full-Time
- Step 2** Click **Add New**. The VLAN ID #2 page appears.
- Step 3** Make the following entries on this page:
- a. VLAN Name: Full-Time
 - b. VLAN Enable: Enabled
 - c. Default Priority: default
 - d. Default policy group: [0] None
 - e. Enhanced MIC verification for WEP: None
 - f. Temporal Key Integrity Protocol: Cisco
 - g. WEP Key Rotation Interval: 0
 - h. Alert?: no
 - i. WEP Key 1: Enter 26 hexadecimal characters.
 - j. Key Size: 128 bit
- Step 4** Click **OK** to save your settings and return to the VLAN Setup page.
- Step 5** Create the Part-Time VLAN using the same settings as Full-Time with the following exceptions:
- a. VLAN ID: 3
 - b. VLAN Name: Part-Time
- Step 6** Click **Add New**. The VLAN ID #3 page appears.
- Step 7** Make the same entries for this page as you did for the Full-Time VLAN.
- Step 8** Click **OK** to save your settings and return to the VLAN Setup page.
-

Creating the Guest VLAN

-
- Step 1** Create a “Guest” VLAN using the following configuration:
- VLAN (802.1Q) Tagging: Disabled
 - Native VLAN ID: 0
 - Single VLAN ID which allows Unencrypted packets: 0
 - Optionally allow Encrypted packets on the unencrypted VLAN: yes
 - VLAN ID: 4
 - VLAN Name: Guest
- Step 2** Click **Add New**. The VLAN ID #4 page appears.
- Step 3** Make the following entries on this page:
- VLAN Name: Guest
 - VLAN Enable: Enabled
 - Default Priority: default
 - Default Policy Group: [0] None
 - Enhanced MIC verification for WEP: None
 - Temporal Key Integrity Protocol: None
 - WEP Key Rotation Interval: 0
 - Alert?: no
 - WEP Key (1- 4): No entry
-  **Note** Apply a policy group (set of L2, L3, and L4 filters) for this VLAN.
-
- Step 4** Click **OK** to save your settings and return to the VLAN Setup page.
- Step 5** On the VLAN Setup page, identify your Guest VLAN (4) in the Single VLAN ID that allows **Unencrypted** packets field and set the Optionally allow **Encrypted** packets on the unencrypted VLAN to **Yes**.
-

Creating the Maintenance VLAN

- Step 6** Add an encrypted VLAN using the following configuration:
- VLAN (802.1Q) Tagging: Disabled
 - Native VLAN ID: 0
 - Single VLAN ID which allows Unencrypted packets: 0
 - Optionally allow Encrypted packets on the unencrypted VLAN: no
 - VLAN ID: 5
 - VLAN Name: Maintenance
- Step 7** Click **Add New**. The VLAN ID #5 page appears.

- Step 8** Make the following entries on this page:
- VLAN Name: Maintenance
 - VLAN Enable: Enabled
 - Default Priority: default
 - Default policy group: [0] None
 - Enhanced MIC verification for WEP: None
 - Temporal Key Integrity Protocol: None
 - WEP Key Rotation Interval: 0
 - Alert?: no
 - WEP Key 1: Set a 128-bit key.
- Step 9** Click **OK** to return to the VLAN Setup page.
- Step 10** Verify that your VLANs are listed in the Existing VLANs field.

Creating and Configuring the SSIDs

After you create the VLANs for your access point, you create the SSIDs to which the VLANs associate. Follow these steps to create the SSIDs.

- Step 1** Click **Setup** to return to the Setup page.
- Step 2** Click **Service Sets**. The AP Radio Service Sets page appears (Figure 4-8).

Figure 4-8 AP Radio Service Sets Page

The screenshot shows the 'AP Radio Service Sets' page with a navigation bar at the top containing links: Home, Map, Network, Associations, Setup, Logs, and Help. The 'Setup' link is highlighted. To the right of the navigation bar, it says 'Uptime: 13 days, 17:41:13'. Below the navigation bar is the title 'Service Set Summary Status'. The main content area includes the following fields and controls:

- Device:** A text input field.
- SSID for use by Infrastructure Stations (such as Repeaters):** A text input field.
- Disallow Infrastructure Stations on any other SSID:** Radio buttons for 'yes' and 'no', with 'no' selected.
- Service Set ID(SSID):** A text input field followed by an 'Add New' button.
- Existing SSIDs:** A list box containing '[0] repeatermania(primary)'. To the right of the list box are 'Edit' and 'Remove' buttons.
- At the bottom of the page are four buttons: 'Apply', 'OK', 'Cancel', and 'RestoreAll'.

61751

- Step 3** In the Existing SSIDs field, highlight the tsunami (primary) SSID and click **Edit**. The AP Radio Primary SSID page appears (Figure 4-9).

Figure 4-9 AP Radio Primary SSID Page

Uptime: 2 days, 02:37:54

Map Help

Device: AP Radio

Service Set ID (Primary SSID): Native VLAN

Current Number of Associations: 0

Maximum Number of Associations: 0

Classify Workgroup Bridges as Network Infrastructure: ☒ yes ☐ no

Default VLAN ID: [1] Native VLAN

Accept Authentication Type:

Require EAP:

Default Unicast Address Filter:

Open Shared Network-EAP

☐ ☒ ☒

☐ ☐ ☐

Allowed Allowed Allowed

To require static or server-based MAC-Address authentication, set "Default Unicast Address Filter" to "Disallowed".

Apply OK Cancel Restore Defaults

- Step 4** Make the following changes to this page:
- Rename the Primary SSID to Native VLAN.
 - Maximum under of Associations: 0
 - Default VLAN ID: [1] Native VLAN.



Note Associating the Default VLAN ID to the native VLAN field is known as mapping the VLAN to the SSID. The mapping process is how the access point is able to “connect” to the VLAN on the switch.

- Classify Workgroup Bridges as Network Infrastructure: yes
- Accept Authentication Type: Shared and Network EAP
- Default Unicast Address Filter: Allowed for each authentication type.

- Step 5** Click **OK**. The AP Radio Service Sets page appears.

- Step 6** In the Service Set ID (SSID) field, enter **full-time** and click **Add New**. The AP Radio SSID #1 page appears (Figure 4-11).

- Step 7** Map the full-time SSID to the full-time VLAN ID by following these steps:

- Highlight the full-time SSID.
- In the VLAN ID drop-down menu, select [2] **full-time** VLAN ID.

- Step 8** Select Network-EAP authentication type and allow default unicast address filters.

- Step 9** Click **OK** to save your settings and return to the AP Radio Service Sets page.

- Step 10** In the Service Set ID (SSID) field, enter Part-Time and click **Add New**. The AP Radio SSID #2 page appears.
- Step 11** Map the Part-Time SSID to the [3] Part-Time VLAN ID.
- Step 12** Select Network-EAP authentication type and allow default unicast address filters.
- Step 13** Click **OK** to save your settings and return to the AP Radio Service Sets page.
- Step 14** Create the Guest SSID and map it to the [4] Guest Default VLAN ID.
- Step 15** Select Open authentication type and allow default unicast address filters.
- Step 16** Click **OK** to save your settings and return to the AP Radio Service Sets page.
- Step 17** Create the Maintenance SSID and map it to the [5] Maintenance Default VLAN ID.
- Step 18** Select Open authentication type and Disallow default unicast address filters.



Note Selecting **Disallow** in this field allows the maintenance hand-held devices to use MAC authentication.

- Step 19** Click **OK** to save your settings and return to the AP Radio Service Sets page.
-

Enabling VLAN (802.1Q) Tagging and Identifying the Native VLAN

When you have finished creating and configuring the VLANs and their associated SSIDs, you must enable VLAN IEEE 802.1Q tagging to make them operational. You must also identify the native VLAN. Follow these steps to enable VLAN IEEE 802.1Q tagging and identify the native VLAN.

-
- Step 1** Browse to the Summary Status page and click **VLAN** in the Associations section. The VLAN Setup page appears (Figure 4-10).

Figure 4-10 VLAN Setup Page

Home Map Network Associations Setup Logs Help Uptime: 2 days, 21:31:29

VLAN (802.1Q) Tagging: ☐ Enabled ☒ Disabled

802.1Q Encapsulation Mode: --Disabled--

Maximum Number of enabled VLAN IDs: 16

Native VLAN ID:

Single VLAN ID which allows **Unencrypted** packets: (0=all require encryption)

Optionally allow **Encrypted** packets on the unencrypted VLAN: ☒ yes ☐ no

VLAN ID: VLAN Name: Add New

Existing VLANs:

1	Native VLAN
2	Full-Time
3	Part-Time
4	Guest
5	Maintenance
When VLAN Disabled	

Edit Remove

Apply OK Cancel RestoreAll

- Step 2** Verify that the VLANs you created appear in the Existing VLANs field.
- Step 3** Click **Cancel** to return to the Setup page.
- Step 4** Click **Service Sets**. The AP Radio Service Sets page appears (Figure 4-11).

Figure 4-11 AP Radio Service Sets Page

Home Map Network Associations Setup Logs Help Uptime: 2 days, 21:36:35

Device: AP Radio

SSID for use by Infrastructure Stations (such as Repeaters):

Disallow Infrastructure Stations on any *other* SSID: ☐ yes ☒ no

Service Set ID(SSID): Add New

Existing SSIDs:

[0]	Native VLAN(primary)
[1]	Full-Time
[2]	Part-Time
[3]	Guest
[4]	Maintenance

Edit Remove

Apply OK Cancel RestoreAll

- Step 5** Verify that the SSIDs you created appear in the Existing SSIDs field.
- Step 6** If the VLANs and SSIDs verified in Steps 2 and 5 are correct, go to Step 7. If not, review the procedures and correct the problem.
- Step 7** In the VLAN (802.1Q) field, click **Enable**.
- Step 8** In the Native VLAN ID field, enter 1.
- Step 9** Click **OK**. The 802.1Q Encapsulation Mode setting changes from Disabled to Hybrid Trunk.
-

Your wireless network is ready to operate using the VLANs you have created.

Creating an SSID for Infrastructure Devices

You must map the native VLAN to an SSID for infrastructure devices (such as workgroup bridges and repeaters) so that they can communicate in the VLAN environment. Follow these steps.

-
- Step 1** From the Setup page, click **Service Sets**.
- Step 2** Create a new SSID called *Infrastructure*.
- Step 3** Return to the AP Radio Service Sets page. Highlight the Infrastructure SSID in the Existing SSIDs field.
- Step 4** In the Disallow Infrastructure Stations on any *other* SSID field, click **Yes**..

Rules and Guidelines for Wireless VLAN Deployment

You may want to consider these rules and guidelines before you deploy wireless VLANs on your network:

- The switch must be capable of providing an IEEE 802.1Q trunk between it and the access point.
- A maximum of 16 VLANs per ESS are supported; each wireless VLAN is represented with a unique SSID.
- Each VLAN must be configured with a unique encryption key.
- Only one unencrypted VLAN per ESS is permitted.
- Only one primary SSID per ESS is supported.
- TKIP/MIC/Broadcast key rotation can be enabled for each VLAN.
- Open, Shared-Key, MAC, Network-EAP (LEAP), and EAP configuration types can be configured on each SSID.
- Shared-Key authentication is supported only on the SSID mapped to the native VLAN (this is most likely to be the Infrastructure SSID).
- A unique policy group (a set of Layer 2, Layer 3, and Layer 4 filters) is allowed for each VLAN.
- Each SSID is mapped to a default wired VLAN with an ability to override its SSID to VLAN ID using RADIUS-based VLAN access control mechanisms.
- RADIUS-based VLAN ID assignment per user is supported.
- RADIUS-based SSID access control per user is supported.
- Assigning a CoS mapping per VLAN is permitted (8 priority levels are supported).

- The number of clients per SSID is controllable.
- All access points and bridges in the same ESS must use the same native VLAN ID in order to facilitate IAPP communication between them.

Wireless LAN security policies can be mapped to the wired LAN switches and routers.



Configuring Filters and Quality of Service

This chapter provides information and configuration procedures for setting up filters. The chapter also provides information and procedures for setting up QoS using filters you create.

This chapter contains the following sections:

- Filter Setup, page 5-2
- QoS Configuration, page 5-10
- Applying QoS, page 5-12
- A Wireless QoS Deployment Example, page 5-17

Filter Setup

This section describes how to set up filtering to control the flow of data through the access point. You can filter data based on protocols and MAC addresses. Each type of filtering is explained in the following sections:

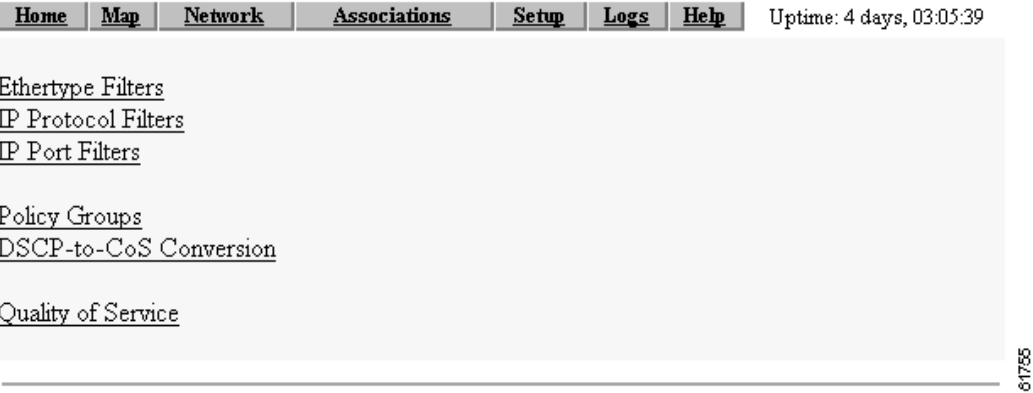
- Protocol Filtering, page 5-2
- MAC Address Filtering, page 5-6

Protocol Filtering

Protocol filters prevent or allow the use of specific protocols through the access point. You can set up individual protocol filters and enable each filter for one or more VLANs. You can filter protocols for wireless client devices, users on the wired LAN, or both. For example, an SNMP filter on the access point's radio port prevents wireless client devices from using SNMP with the access point but does not block SNMP access from the wired LAN.

Use the Protocol Filters Setup page create and enable protocol filters for the access point's Ethernet port and for the access point's radio port. The Protocol Filters Setup page is shown on Figure 5-1.

Figure 5-1 Protocol Filters Setup Page



Follow this link path to reach the Protocol Filters Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Protocol Filters** in the Protocol Filters row under Associations.

You can create protocol filters or view existing filters by clicking **Filters** in the Ethernet or Radio rows of the Network Ports section of the Setup page. The screens are identical except for the name. Figure 5-2 shows the Protocol Filters page.

Figure 5-2 Protocol Filters Page

Follow this link path to reach the AP Radio or Ethernet Protocol Filters page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Filters** in the AP Radio or Ethernet row under Network Ports.

The left side of the Protocol Filters page contains links to the EtherType Filters, the IP Protocol Filters, and the IP Port Filters pages.

Use the Protocol Filters pages to assign protocols to a filter set. Table B-1, Table B-2, and Table B-3 in Appendix B list the protocols available on each page.

Creating a Protocol Filter

Follow these steps to create a protocol filter:

- Step 1** Follow the link path to the Protocol Filters Setup page.
- Step 2** Click **Ethertype**, **IP Protocol**, or **IP Port** to display the Filters page that contains the protocols you want to filter. Figure 5-3 shows the IP Protocol Filters page.

Figure 5-3 IP Protocol Filters Page

- Step 3** Enter a descriptive filter set name in the Set Name field.
- Step 4** Enter an identification number in the Set ID entry field if you want to assign a specific SNMP identifier to the filter set. If you don't enter an ID, an SNMP identifier will be assigned to the set automatically, starting with 1 for the first filter set and incrementing by one for each additional set.
- Step 5** Click **Add New**. The Filter Set page appears. Figure 5-4 shows the Filter Set page.

Figure 5-4 Filter Set Page

Map Help Uptime: 01:11:36

Name: test17

Default Disposition: forward

Default Time To Live (msec):
unicast: 0 multicast: 0

Special Cases: Add New

Select an entry from below to or

				Time-to-Live (msec)		
select	Ethertype	Disposition	Priority	Unicast	Multicast	Alert?

- Step 6** Select **forward** or **block** from the Default Disposition drop-down menu. This setting is the default action for the protocols you include in the filter set. You can override this setting for specific protocols.
- Step 7** In the Default Time to Live fields, enter the number of milliseconds unicast and multicast packets should stay in the access point's buffer before they are discarded. These settings will be the default time-to-live values for the protocols you include in the filter set, but you can override the settings for specific protocols. If you leave these settings at 0, the time-to-live settings default to 3 seconds for multicast packets and 5 seconds for unicast packets.
- Step 8** Type the name or the ISO numeric designator for the protocol you want to add in the Special Cases entry field and click **Add New**. For example, to add Telnet to an IP port filter set, type **telnet** or **23**.

The Protocol Filter Set page appears. Figure 5-5 shows the Protocol Filter Set page.

Figure 5-5 Protocol Filter Set Page

Map Help Uptime: 01:50:27

Name:

Default Disposition: forward

Default Time To Live (msec):
unicast: 0 multicast: 0

Special Cases: Add New

Select an entry from below to or

				Time-to-Live (msec)		
select	IP Protocol	Disposition	Priority	Unicast	Multicast	Alert?

- Step 9** Select **forward** or **block** from the Disposition drop-down menu to forward or block the protocol traffic, or leave this setting at **default** to use the default disposition that you selected for the filter set in Step 6.
- Step 10** Select a priority for the protocol from the Priority drop-down menu. The menu includes the following options:
- **background**—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications.
 - **default**—This setting is the same as best effort, which applies to normal LAN traffic.
 - **excellentEffort**—Use this setting for a network’s most important users.
 - **controlledLoad**—Use this setting for important business applications that are subject to some form of admission control.
 - **interactiveVideo**—Use this setting for traffic with less than 100 ms delay.
 - **interactiveVoice**—Use this setting for traffic with less than 10 ms delay.
 - **networkControl**—Use this setting for traffic that must get through to maintain and support the network infrastructure.
- Step 11** Enter milliseconds in the Time-to-Live entry fields. If you leave these settings at 0, the protocol adopts the default time-to-live values you entered in Step 7.

**Note**

The time-to-live values you enter should be compatible with the priority you select for the protocol. For example, if you select **interactiveVoice** as the priority and enter high time-to-live values, voice packets will stay in the access point buffer longer than necessary, causing delivery of stale, useless packets.

- Step 12** Select *Alert?* **yes** to send an alert to the event log when a user transmits or receives the protocol through the access point.
- Step 13** Click **OK**. The Filter Set page appears with the protocol listed at the bottom of the page.
- To edit the protocol entry, type the protocol name in the Special Cases entry field or click the select button beside the entry and click **Edit**. To delete the protocol, type the protocol name in the Special Cases entry field or click the select button beside the entry and click **Remove**.
- Step 14** To add another protocol to the filter set, repeat Step 8 through Step 13. When you have included all the protocols you need in the filter set, click **OK**. The EtherType Filters, IP Protocol Filters, or IP Port Filters page appears, and the filter sets you defined appear in the filter set list at the bottom of the page.

**Note**

After defining the protocol filter set, follow the steps in the Enabling a Protocol Filter section to activate the filter.

Enabling a Protocol Filter

Follow these steps to enable a protocol filter:

- Step 1** Complete the steps listed in the “Creating a Protocol Filter” section on page 5-3 to define a protocol filter.
- Step 2** Follow the link path to the Ethernet Protocol Filters page or the AP Radio Protocol Filters page.

- Step 3** Select the protocol filter set that you want to enable from the Ethertype, IP Protocol, or IP Port drop-down menu.
- Step 4** Click **OK**. The filter set is enabled.

MAC Address Filtering

MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify.



Note

MAC address filters are powerful, and you can lock yourself out of the access point if you make a mistake setting up the filters. If you accidentally lock yourself out of your access point, follow the instructions in the “Using the Command-Line Interface” section on page 2-19 to use the CLI to disable the filters.

Use the Address Filters page to create MAC address filters for the access point. Figure 5-6 shows the Address Filters page.

Figure 5-6 Address Filters Page

Map Help Uptime: 6 days, 22:56:46

New MAC Address Filter:

Dest MAC Address:

☒ Allowed ☐ Disallowed

The default settings for multicast and unicast destination MAC addresses transmitted from each network interface are specified on the Advanced Setup page for that network interface.

Existing MAC Address Filters:

Lookup MAC Address on Authentication Server if not in Existing Filter List? ☐ yes ☒ no

Is MAC Authentication alone sufficient for a client to be fully authenticated? ☐ yes ☒ no

43993

Follow this link path to reach the Address Filters page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Address Filters** under Associations.

Creating a MAC Address Filter

Follow these steps to create a MAC address filter:

Step 1 Follow the link path to the Address Filters page.

Step 2 Type a destination MAC address in the New MAC Address Filter: Dest MAC Address field. You can type the address with colons separating the character pairs (00:40:96:12:34:56, for example) or without any intervening characters (004096123456, for example).



Note If you plan to disallow traffic to all MAC addresses except those you specify as allowed, put your own MAC address in the list of allowed MAC addresses. If you plan to disallow multicast traffic, add the broadcast MAC address (ffffffffff) to the list of allowed addresses.

Step 3 Click **Allowed** to pass traffic to the MAC address or click **Disallowed** to discard traffic to the MAC address.

Step 4 Click **Add**. The MAC address appears in the Existing MAC Address Filters list. To remove the MAC address from the list, select it and click **Remove**.



Tip

You can create a list of allowed MAC addresses on an authentication server on your network. Consult the “Setting Up MAC-Based Authentication” section on page 8-29 for instructions on using MAC-based authentication.

Step 5 Click **OK**. You return automatically to the Setup page.

Step 6 Click **Advanced** in the AP Radio row of the Network Ports section at the bottom of the Setup page. The AP Radio Advanced page appears. Figure 5-7 shows the AP Radio Advanced page.

Figure 5-7 AP Radio Advanced Page

Map Help Uptime: 3 days, 17:01:17

Requested Status: Up

Current Status: Up

Packet Forwarding: Enabled

Forwarding State: Forwarding

Default Multicast Address Filter: Allowed

Maximum Multicast Packets/Second: 0

Radio Cell Role: Access Point/Root

SSID for use by Infrastructure Stations (such as Repeaters): 0

Disallow Infrastructure Stations on any *other* SSID: ☐ yes ☒ no

Use Aironet Extensions: ☒ yes ☐ no

Classify Workgroup Bridges as Network Infrastructure: ☒ yes ☐ no

Require use of Radio Firmware 4.99H: ☒ yes ☐ no

Ethernet Encapsulation Transform: RFC1042

Quality of Service Setup

If VLANs are *not* enabled, set the following three parameters on this page. If VLANs *are* enabled, the following three parameters are set independently for each enabled VLAN through [VLAN Setup](#).

Enhanced MIC verification for WEP: None

Temporal Key Integrity Protocol: None

Broadcast WEP Key rotation interval (sec): 0 (0=off)

To configure 802.11 Authentication, EAP, Unicast Address Filters, and the Maximum Number of Associations for this radio's Primary SSID (the default SSID), please use the link below.

Advanced Primary SSID Setup

Specified Access Point 1: 00:00:00:00:00:00

Specified Access Point 2: 00:00:00:00:00:00

Specified Access Point 3: 00:00:00:00:00:00

Specified Access Point 4: 00:00:00:00:00:00

Radio Modulation: Standard

Radio Preamble: Short

Apply OK Cancel Restore Defaults

81736

Step 7 Click **Advanced Primary SSID Setup**. The AP Radio Primary SSID page appears. Figure 5-8 shows the AP Radio Primary SSID page.

Figure 5-8 AP Radio Primary SSID Page

Uptime: 3 days, 17:05:21

Map Help

Device: AP Radio

Service Set ID (Primary SSID): SJOLEAP

Maximum Number of Associations: 0

Classify Workgroup Bridges as Network Infrastructure: ☒ yes ☐ no

Proxy Mobile IP is enabled: ☐ yes ☒ no

Default VLAN ID: [0] -None-

Default Policy Group ID: [0] -None-

Accept Authentication Type:

Open	Shared	Network-EAP
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	
Allowed	Allowed	Allowed

Default Unicast Address Filter:

To require static or server-based MAC-Address authentication, set "Default Unicast Address Filter" to "Disallowed".

Apply OK Cancel Restore Defaults

Select **Open**, **Shared Key**, or **Network-EAP** to set the authentications the access point recognizes. See the “Security Overview” section on page 7-2 for a description of authentication types.

If you use open or shared authentication as well as EAP authentication, select **Require EAP** under Open or Shared to block client devices that are not using EAP from authenticating through the access point.

Unicast MAC address filters allow or disallow the forwarding of unicast packets sent to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify.

Read the “Setting Up MAC-Based Authentication” section on page 7-29 for complete instructions on using MAC-based authentication on an authentication server. Read the “Creating a MAC Address Filter” section on page 5-7 for complete instructions on setting up MAC address filters.

The drop-down menus for unicast address filters contain two options:

- **Allowed**—The access point forwards all traffic except packets sent to the MAC addresses listed as disallowed on the Address Filters page.
- **Disallowed**—The access point discards all traffic except packets sent to the MAC addresses listed as allowed on the Address Filters page or on your authentication server.

Select **Disallowed** for each authentication type that also uses MAC-based authentication.



Note If you plan to discard traffic to all MAC addresses except those you specify (the Disallowed setting), be sure to enter your own MAC address as allowed on the Address Filters page or on your authentication server.

Step 8 Click **OK**. Your settings are saved and you return to the AP Radio Advanced Setup page.

If clients are not filtered immediately, click **WARM RESTART SYSTEM NOW** on the Manage System Configuration page to restart the access point. To reach the Manage System Configuration page, Click **Cisco Services** on the main Setup page and click **Manage System Configuration** on the Cisco Services Setup page.

**Note**

The Ethernet Advanced page contains the Default Unicast and Multicast Address Filter settings for the Ethernet port. These settings work as described above, but you should use extra caution changing the settings on the Ethernet Advanced page because they can lock you out of your access point. To reach the Ethernet Advanced page, click **Advanced** in the Ethernet row of the Network Ports section at the bottom of the Setup page.

**Note**

Client devices with blocked MAC addresses cannot send or receive data through the access point, but they might remain in the Association Table as unauthenticated client devices. Client devices with blocked MAC addresses disappear from the Association Table when the access point stops monitoring them or they associate with another access point. See the “Association Table Advanced Page” section on page 7-16 for information on setting a monitoring timeout for each device class.

QoS Configuration

You can assign QoS attributes to enable various devices on the network to communicate more effectively. The access point or bridge supports QoS for voice over IP (VoIP) telephones and downlink prioritized channel access for streaming audio and video traffic. This section describes how to configure the access point's or bridge's QoS feature.

Entering Information on the Quality of Service Setup Page

Access the Quality of Service Setup page (see Figure 5-9) from the Summary Status page by clicking the **Setup** tab. From the Associations section of the Setup page, click **Protocol Filters**. This page is also accessed through the AP Radio Advanced page in the Network Ports section of the Setup page.

Figure 5-9 Quality of Service Setup Page

Map Help Uptime: 3 days, 19:05:33

Generate QBSS Element: ☐ yes ☒ no

Use Symbol Extensions: ☐ yes ☒ no

Send IGMP General Query: ☐ yes ☒ no

Traffic Category	CWmin	CWmax
1: Background	31	255
2: (spare)	31	255
0: Best Effort (default)	31	255
3: Excellent Effort	31	255
4: Controlled Load	15	255
5: Interactive Video	15	63
6: Interactive Voice	3	31
7: Network Control	7	127

Allowed values for CWmin and CWmax are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023.
CWmin must be less than or equal to CWmax.

Apply OK Cancel Restore Defaults

Follow this link path to reach the Quality of Service setup page:

1. On the Summary Status page, click **Setup**. The Setup page appears.
2. In the Associations section, click **Protocol Filters**. The Protocol Filters Setup page appears.
3. Click **Quality of Service**. The AP Radio Quality of Service page appears.

Settings on the Quality of Service Setup Page

The Quality of Service setup page contains the following settings:

- Generate QBSS Element
- Use Symbol Extensions
- Send IGMP General Query
- Traffic Category

Generate QBSS Element

Determines whether a QoS basic service set (QBSS) element is generated. The QBSS element determines the best access point with which to associate.

Use Symbol Extensions

Configures the access point to use Symbol Voice over IP (VoIP) phones. When this setting is enabled, the access point uses the Symbol Phone Support protocol. This protocol identifies Symbol handsets and classifies traffic for them as interactive voice.

Send IGMP General Query

Configures the access point to perform IP multicast filtering on behalf of its clients. When Internet Group Membership Protocol (IGMP) snooping is enabled on a switch, and a client roams from one access point to another, the multicast session is dropped. Enabling this feature causes the access point to send a general IGMP query to the network infrastructure on behalf of the client every time it associates or reassociates to the access point. By doing so, the multicast stream is maintained for the client as it roams.

Traffic Category

Traffic category identifies a type of traffic in which data processed by the access point is categorized. There are seven categories:

- Background
- Spare
- Best effort
- Excellent effort
- Controlled load
- Interactive video
- Interactive voice
- Network control

Each category is assigned a minimum contention window (CWmin) value and a maximum contention window (CWmax) value. Allowed values for CWmin and CWmax are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023.

**Note**

Cisco recommends that you do not alter these settings without significant testing. If you do alter the values, CWmin must be less than or equal to CWmax.

Applying QoS

You can apply QoS to specific traffic handled by the access point or bridge in a number of ways:

- By station
- By VLAN
- By filter
- By Class of Service (CoS) value
- By differentiated services code point (DSCP) value

By Station

The access point or bridge can prioritize traffic based upon a WLAN client identifying itself as a particular client type that requires a particular traffic classification.

The best example of this is the negotiations between the access point and a Symbol VoIP WLAN handset. A protocol has been defined by Symbol that allows the handset to be identified by the access point and given interactive voice classification. Follow these steps to enable this feature.

- Step 1** Browse to the Setup screen on the access point.
- Step 2** Click **Protocol Filters** in the Associations section. The Protocol Filters Setup page appears (Figure 5-10).

Figure 5-10 Protocol Filters Setup Page

Home Map Network Associations Setup Logs Help Uptime: 4 days, 03:05:39

Ethertype Filters
IP Protocol Filters
IP Port Filters

Policy Groups
DSCP-to-CoS Conversion

Quality of Service

- Step 3** Click **Quality of Service**. The AP Radio Quality of Service page appears (Figure 5-11).

Figure 5-11 AP Radio Quality of Service Page

Map Help Uptime: 3 days, 19:05:33

Generate QBSS Element: ☐ yes ☒ no
 Use Symbol Extensions: ☐ yes ☒ no
 Send IGMP General Query: ☐ yes ☒ no

Traffic Category	CWmin	CWmax
1: Background	31	255
2: (spare)	31	255
0: Best Effort (default)	31	255
3: Excellent Effort	31	255
4: Controlled Load	15	255
5: Interactive Video	15	63
6: Interactive Voice	3	31
7: Network Control	7	127

Allowed values for CWmin and CWmax are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023.
 CWmin must be less than or equal to CWmax.

Apply OK Cancel Restore Defaults

Step 4 Click the **yes** radio button in the Use Symbol Extensions setting.

By VLAN

The default priority of a VLAN can be set, and the access point or bridge uses this setting for all traffic on that VLAN except when overridden by a filter setting. This filter setting is applied through the policy group on the VLAN.

Follow these steps to set up a VLANs QoS default priority.

Step 1 From the Setup page, click **VLAN** in the Associations section. The VLAN Setup page appears.

Step 2 Choose the VLAN to which you want to apply the priorities by highlighting it in the Existing VLANs field, and click **Edit**. The VLAN ID page for that VLAN appears (Figure 5-12).

Figure 5-12 VLAN ID page

[Map](#)
[Help](#)

Uptime: 4 days, 03:23:12

VLAN Name:
VLAN Enable:
Default Priority:
Default Policy Group:
Enhanced MIC verification for WEP:
Temporal Key Integrity Protocol:
WEP Key Rotation Interval:
Alert?:

Full-Time

☒ Enabled
☐ Disabled

default

Background
Spare
default
Excellent Effort
Controlled Load
Interactive Video
Interactive Voice
Network Control

Encryption Key

Key Size

WEP Key 1:

WEP Key 2:

WEP Key 3:

WEP Key 4:

128 bit

not set

not set

not set

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).

Apply

OK

Cancel

Restore Defaults

Step 3 To view the selections in the Default Priority field, click the drop-down menu.

Step 4 Select the default priority you wish the VLAN to use.

Step 5 Click **OK** to save your settings and return to the VLAN Setup page.

By Filter

Access point and bridge filters already allow the classification of traffic based upon Ethertype, Internet Protocol, or IP Port. An example of a filter classifying traffic is shown on Figure 5-13.

Figure 5-13 Filters Priority Setting

Uptime: 00:23:36

Disposition: default

Priority: Interactive Voice

Unicast Time-to-Live (msec):

Multicast Time-to-Live (msec):

Alert?:

Apply OK Restore Defaults

The filters can be applied on interfaces or as a part of a VLAN policy group.

The access point has a default filter to classify all Spectralink voice traffic with voice priority. You do not have to enable this filter, but you can modify the filter and apply it to a specific VLAN or interface.



Note

To set up a filter, see the “Filter Setup” section on page 5-2.

A typical Spectralink filter configuration is shown on Figure 5-14.

Figure 5-14 Spectralink Filter Configuration

Uptime: 00:14:29

Name: Voice Over IP

Default Disposition: forward

Default Time To Live (msec):

unicast: 0 multicast: 0

Special Cases: Add New

Select an entry from below to Edit or Remove

select	IP Protocol	Disposition	Priority	Time-to-Live (msec)		Alert?
				Unicast	Multicast	
<input type="radio"/>	[SVP] 0x0077	default	interactiveVoice	0	0	

Apply OK Cancel Restore Defaults

Figure 5-15 shows how the Spectralink filter is applied.

Figure 5-15 Applying the Spectralink Filter

By CoS Value

Traffic that comes to the access point or bridge over an Ethernet trunk is already classified by its Class of Service (CoS) settings. The classification is applied unless changed by one of the methods described above.

By DSCP Value

The differentiated services code point (DSCP) values in the IP packets can be used to classify the traffic based on the DSCP-to-CoS mappings shown in Figure 5-16.

Figure 5-16 DSCP-to-CoS Conversion

DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS
0	Best Effort	16	Spare	32	Controlled Load	48	Interactive Voice
1	No Change	17	No Change	33	No Change	49	No Change
2	No Change	18	Spare	34	Controlled Load	50	No Change
3	No Change	19	No Change	35	No Change	51	No Change
4	No Change	20	No Change	36	No Change	52	No Change
5	No Change	21	No Change	37	No Change	53	No Change
6	No Change	22	No Change	38	No Change	54	No Change
7	No Change	23	No Change	39	No Change	55	No Change
8	Background	24	Excellent Effort	40	Interactive Video	56	Network Control
9	No Change	25	No Change	41	No Change	57	No Change
10	Background	26	Excellent Effort	42	No Change	58	No Change
11	No Change	27	No Change	43	No Change	59	No Change
12	No Change	28	No Change	44	No Change	60	No Change
13	No Change	29	No Change	45	No Change	61	No Change
14	No Change	30	No Change	46	Interactive Video	62	No Change
15	No Change	31	No Change	47	No Change	63	No Change

Follow these steps to access the DSCP-to-CoS Conversion page.

-
- Step 1** From the Summary Status page, click **Setup**. The Setup page appears.
- Step 2** In the Associations section, click **Protocol Filters**. The Protocol Filters Setup page appears.
- Step 3** Click **DSCP-to-CoS Conversion**.
-

A Wireless QoS Deployment Example

This section outlines a typical use for deploying QoS on a wireless LAN: configuring the access point or bridge to properly prioritize an 802.11b wireless phone using a VLAN.

Before discussing the steps involved to configure this QoS scenario, it is assumed that you have configured and enabled VLANs on the access point and that all downstream interactive voice configurations are made to other infrastructure devices and applicable applications on the wired LAN, such as switches, routers, DHCP servers, Call Manager, etc.

In this example, we create a VLAN dedicated to interactive voice. Its ID is 12 and its name is *Voice*. An SSID called *Voice* is created to handle the interactive voice traffic on the access point.



Note

The example shows how to configure QoS on a root access point. Screens will differ slightly for repeater access points and bridged applications.

Follow these steps to configure the access point:

-
- Step 1** Browse to the Setup screen on the access point.
- Step 2** In the Associations section, click **VLAN**. The VLAN Setup page appears.
- Step 3** Enter a VLAN ID in the VLAN ID field.
- Step 4** Enter a VLAN name in the VLAN Name field (Figure 5-17).

Figure 5-17 VLAN Setup page

Home Map Network Associations Setup Logs Help Uptime: 9 days, 01:27:48

VLAN Summary Status

VLAN (802.1Q) Tagging: ☐ Enabled ☒ Disabled
 802.1Q Encapsulation Mode: --Disabled--
 Maximum Number of enabled VLAN IDs: 16
 Native VLAN ID:
 Single VLAN ID which allows **Unencrypted** packets: (0=all require encryption)
 Optionally allow **Encrypted** packets on the unencrypted VLAN: ☐ yes ☒ no

VLAN ID: VLAN Name:

Existing VLANs:

When VLAN Disabled

- Step 5** Click **Add New**. The VLAN ID #xx page appears.
- Step 6** Set VLAN Enable setting to **Enable**.
- Step 7** In the Default Priority Group drop-down menu, select **Interactive Voice**. (Figure 5-18).

Figure 5-18 VLAN ID #xx page

Map Help Uptime: 9 days, 01:39:03

VLAN Name:
 VLAN Enable: ☒ Enabled ☐ Disabled
 Default Priority:
 Default Policy Group:
 Enhanced MIC verification for WEP:
 Temporal Key Integrity Protocol:
 WEP Key Rotation Interval: (0=off)
 Alert?: ☐ yes ☒ no

	Encryption Key	Key Size
WEP Key 1:	<input type="text"/>	<input type="text" value="not set"/>
WEP Key 2:	<input type="text"/>	<input type="text" value="not set"/>
WEP Key 3:	<input type="text"/>	<input type="text" value="not set"/>
WEP Key 4:	<input type="text"/>	<input type="text" value="not set"/>

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
 Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).

**Note**

Wireless phones do not support Enhanced MIC verification for WEP or TKIP. No changes are required for these settings.

If your wireless phone has a WEP key set, go to the next section. If a WEP key is not set, go to the “WEP Not Set on the Wireless Phone” section on page 5-19.

WEP Set on the Wireless Phone

If WEP is set on your wireless phone, you must set an identical WEP key for the interactive voice VLAN. Follow these steps to set the WEP key.

- Step 1** Enter the phone’s WEP key in the WEP Key 1 Encryption Key field.
- Step 2** In the Key Size drop-down menu, select the WEP key size set on the phone.
- Step 3** Click **Apply** or **OK**. The configuration is complete.

WEP Not Set on the Wireless Phone

If a WEP key is not set on the wireless phone, you must complete the configuration by following these steps:

- Step 1** Browse to the VLAN Setup page.
- Step 2** In the Single VLAN ID which allows **Unencrypted** packets field, enter the Voice VLAN ID.
- Step 3** Set the Optionally allow **Encrypted** packets on the unencrypted VLAN to **yes** (Figure 5-19).

Figure 5-19 VLAN Setup page

Home Map Network Associations Setup Logs Help Uptime: 9 days, 02:00:49

VLAN Summary Status

VLAN (802.1Q) Tagging: ☐ Enabled ☒ Disabled

802.1Q Encapsulation Mode: --Disabled--

Maximum Number of enabled VLAN IDs: 16

Native VLAN ID: 0

Single VLAN ID which allows **Unencrypted** packets: 12 (0=all require encryption)

Optionally allow **Encrypted** packets on the unencrypted VLAN: ☒ yes ☐ no

VLAN ID: VLAN Name:

Existing VLANs:

12 Voice *When VLAN Disabled*	<input type="button" value="Edit"/> <input type="button" value="Remove"/>
----------------------------------	--

- Step 4** Click **OK**. You are returned to the Setup page.
- Step 5** In the Associations section, click **SSIDs: Int**. The AP Radio: Internal Service Sets page appears.
- Step 6** Enter a valid SSID in the Service Set ID (SSID) field (Figure 5-20).

Figure 5-20 AP Radio: Internal Service Sets page

Home Map Network Associations Setup Logs Help Uptime: 9 days, 02:05:59

Service Set Summary Status

Device: AP Radio: Internal

SSID for use by Infrastructure Stations (such as Repeaters): 0

Disallow Infrastructure Stations on any other SSID: ☐ yes ☒ no

Service Set ID(SSID): Voice Add New

Existing SSIDs:

[0] TestAP 2(primary)

Edit Remove

Apply OK Cancel RestoreAll 86651

- Step 7** Click **Add New**. The AP Radio: Internal SSID #x page appears.
- Step 8** In the Default VLAN ID drop-down menu, select **[12] Voice** (Figure 5-21).

Figure 5-21 AP Radio: Internal Service Sets page

Map Help Uptime: 9 days, 02:09:57

Device: AP Radio: Internal

Service Set ID (SSID): Voice

Current Number of Associations: 0

Maximum Number of Associations: 0

Proxy Mobile IP is enabled: ☐ yes ☒ no

Default VLAN ID: [12] Voice

Default Policy Group ID: [0] -None-

Accept Authentication Type: ☒ Open ☐ Shared ☐ Network-EAP

Require EAP: ☐ Open ☐ Shared ☐ Network-EAP

Default Unicast Address Filter: Allowed Allowed Allowed

To require static or server-based MAC-Address authentication, set "Default Unicast Address Filter" to "Disallowed".

Apply OK Cancel Restore Defaults 86652

- Step 9** Leave all other settings at the default settings and click **OK**. You are returned to the AP Radio: Internal Service Sets page.
- Step 10** Click **OK** again to return to the Setup page.
-

Your configuration is complete.



Configuring Proxy Mobile IP

This chapter describes how to enable and configure your access point's proxy Mobile IP feature. The chapter contains the following sections:

- Proxy Mobile IP, page 6-2
- The Proxy Mobile IP Setup Page, page 6-9
- Configuring Proxy Mobile IP, page 6-19

Proxy Mobile IP

These sections explain how access points conduct proxy Mobile IP:

- Overview, page 6-2
- Components of a Proxy Mobile IP Network, page 6-3
- How Proxy Mobile IP Works, page 6-4
- Proxy Mobile IP Security, page 6-8

Overview

The access point's proxy Mobile IP feature works in conjunction with the Mobile IP feature on Cisco devices on the wired network. When you enable proxy Mobile IP on your access point and on your wired network, the access point helps client devices from other networks remain connected to their home networks. The visiting client devices do not need special software; the access point provides proxy Mobile IP services on their behalf. Any wireless client can participate.

Mobile IP provides users the freedom to roam beyond their home subnets while maintaining their home IP addresses. This enables transparent routing of IP datagrams to mobile users during their movement, so that data sessions can be initiated to them while they roam. For example, a client device with an IP address of 192.95.5.2 could associate to an access point on a network whose IP addresses are in the 209.165.200.x range. The guest client device keeps its 192.95.5.2 IP address, and the access point forwards its packets through a Mobile IP enabled router across the Internet to a router on the client's home network.

Access points with proxy Mobile IP enabled attempt to provide proxy service for any client device that associates and does not perform the following:

- Issue a DHCP request to get a new IP address.
- Support a Mobile IP stack. If a device supports a Mobile IP stack, the access point assumes that the device will perform its own Mobile IP functions.

You enable proxy Mobile IP for specific SSIDs on the access point, providing support only for clients who use those SSIDs. Proxy Mobile IP does not support VLANs.

Proxy Mobile IP is disabled by default.

**Note**

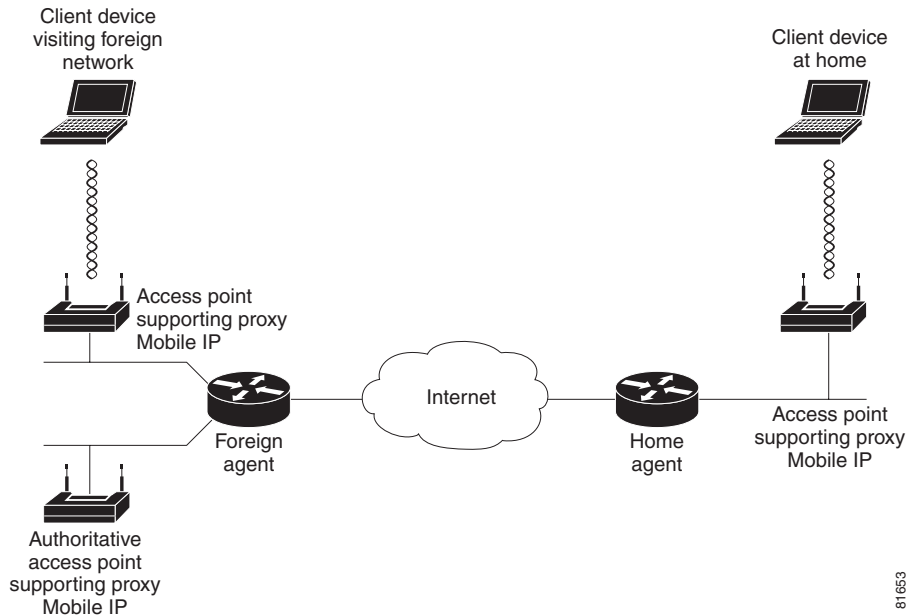
Guest client devices do not receive broadcast and multicast packets from their home networks.

Components of a Proxy Mobile IP Network

Five devices participate in proxy Mobile IP:

- A visiting client device. The visiting client device is any device such as a personal digital assistant or a laptop that can associate to a wireless access point. It does not need any special proxy Mobile IP client software.
- An access point with proxy Mobile IP enabled. The access point proxies on behalf of the visiting client device, performing all Mobile IP functions for the device. The access point uses a subnet map to keep track of home agent information. The access point also gets updates about new home agents from the authoritative access point.
- An authoritative access point on your network supporting proxy Mobile IP. The authoritative access point uses a subnet map to collect and distribute home agent information stored in the subnet map to all the regular access points for all visiting client devices.
- A home agent. The home agent is a router on the visiting client's home network that serves as the anchor point for communication with the access point and the visiting client. The home agent tunnels packets from a correspondent node on the Internet to the visiting client device.
- A foreign agent. The foreign agent is a router on your network that serves as the point of attachment for the visiting client device when it is on your network, delivering packets from the home agent to the visiting client.

Figure 6-1 shows the five participating devices.

Figure 6-1 Participating Devices in Proxy Mobile IP

How Proxy Mobile IP Works

The proxy Mobile IP process has four main phases. These sections describe each phase:

- Agent Discovery, page 6-4
- Subnet Map Exchange, page 6-5
- Registration, page 6-6
- Tunneling, page 6-7

Agent Discovery

During the agent discovery phase, the home agent and the foreign agent advertise their services on the network by using the ICMP Router Discovery Protocol (IRDP). The access point monitors these advertisements.

The IRDP advertisements carry Mobile IP extensions that specify whether an agent is a home agent, foreign agent, or both; its care-of address; the types of services it provides, such as reverse tunneling and generic routing encapsulation (GRE); and the allowed registration lifetime or roaming period for visiting client devices. Rather than waiting for agent advertisements, an access point can send out an agent solicitation. This solicitation forces any agents on the network to immediately send an agent advertisement.

When an access point determines that a client device is connected to a foreign network, it acquires a care-of address for the visiting client. The care-of address is an IP address of a foreign agent that has an interface on the network being visited by a client device. An access point can share this address among many visiting client devices.

When the visiting client associates to an access point, the access point compares the client's IP address with that of its own IP network information and detects that the client is a visitor from another network. The access point then begins the registration. However, before the access point can begin the registration process on behalf of the visiting client, it must have the home agent IP address of the visiting client, which it gets from a subnet map table.

Subnet Map Exchange

Each access point with proxy Mobile IP enabled maintains a subnet map table. The subnet map table consists of a list of home agent IP addresses and their subnet masks. Table 6-1 is an example of a subnet map table.

Table 6-1 Example of a Subnet Map Table

Home Agent	Subnet Mask
10.10.10.1	255.255.255.0
10.10.4.2	255.255.255.0
10.3.4.4	255.255.255.248
10.12.1.1	255.255.0.0

Access points use the subnet map table to determine the IP address of the visiting client's home agent. When an access point boots up or when proxy Mobile IP is first enabled on an access point, it obtains its own home agent information using

the agent discovery mechanism. It sends this information to another access point called an authoritative access point (AAP). The AAP is an access point that maintains the latest subnet map table.

When the AAP receives the new information, it replies to the access point with a copy of the latest subnet map table. The new access point now has the latest subnet map table locally and it is ready to perform proxy Mobile IP for visiting clients. Having the subnet map table locally helps the access point do a quick lookup for the home agent information. Meanwhile, the AAP adds the new access point to its list of access points and the home agent information to its subnet map table. The AAP then updates all the other access points with this additional piece of information.

You can designate up to three AAPs on your wireless LAN. If an access point fails to reach the first AAP, it tries the next configured AAP. The AAPs compare their subnet map tables periodically to make sure they have the same subnet map table. If the AAP detects that there are no more access points for a particular home agent, it sends an invalid registration packet with a bad SPI and group key using the broadcast address of the home agent subnet to determine if the home agent is still active. If the home agent responds, the AAP keeps the home agent entry in the subnet map table even though there are no access points in the home agent's subnet. This process supports client devices that have already roamed to foreign networks. If the home agent does not respond, the AAP deletes the home agent entry from the subnet map table.

When a client device associates to an access point and the access point determines that the client is visiting from another network, the access point performs a longest-match lookup on its subnet map table and obtains the home agent address for the visiting client. When the access point has the home agent address, it can proceed to the registration step.

Registration

The access point is configured with the mobility security association (which includes the shared key) of all potential visiting clients with their corresponding home agents. You can enter the mobility security association information locally on the access point or on a RADIUS server on your network, and access points with proxy Mobile IP enabled can access it there.

The access point uses the security association information, the visiting client's IP address, and the information that it learns from the foreign agent advertisements to form a Mobile IP registration request on behalf of the visiting client. It sends

the registration request to the visiting client's home agent through the foreign agent. The foreign agent checks the validity of the registration request, which includes verifying that the requested lifetime does not exceed its limitations and that the requested tunnel encapsulation is available. If the registration request is valid, the foreign agent relays the request to the home agent.

The home agent checks the validity of the registration request, which includes authentication of the visiting client. If the registration request is valid, the home agent creates a mobility binding (an association of the visiting client with its care-of address), a tunnel to the care-of address, and a routing entry for forwarding packets to the home address through the tunnel.

The home agent then sends a registration reply to the visiting client through the foreign agent (because the registration request was received through the foreign agent). The foreign agent verifies the validity of the registration reply, including ensuring that an associated registration request exists in its pending list. If the registration reply is valid, the foreign agent adds the visiting client to its visitor list, establishes a tunnel to the home agent, and creates a routing entry for forwarding packets to the home address. It then relays the registration reply to the visiting client.

Finally, the access point checks the validity of the registration reply. If the registration reply specifies that the registration is accepted, the access point is able to confirm that the mobility agents are aware of the visiting client's roaming. Subsequently, the access point intercepts all packets from the visiting client and sends them to the foreign agent.

The access point reregisters on behalf of the visiting client before its registration lifetime expires. The home agent and foreign agent update their mobility binding and visitor entry, respectively, during reregistration.

A successful Mobile IP registration by the access point on behalf of the visiting client sets up the routing mechanism for transporting packets to and from the visiting client as it roams.

Tunneling

The visiting client sends packets using its home IP address, effectively maintaining the appearance that it is always on its home network. Even while the visiting client is roaming on foreign networks, its movements are transparent to correspondent nodes (other devices with which the visiting client communicates).

Data packets addressed to the visiting client are routed to its home network, where the home agent intercepts and tunnels them to the care-of address toward the visiting client. Tunneling has two primary functions: encapsulation of the data packet to reach the tunnel endpoint, and decapsulation when the packet is delivered at that endpoint. The tunnel mode that the access point supports is IP Encapsulation within IP Encapsulation.

Typically, the visiting client sends packets as it normally would. The access point intercepts these packets and sends them to the foreign agent, which routes them to their final destination, the correspondent node.

Proxy Mobile IP Security

Mobile IP uses a strong authentication scheme to protect communications to and from visiting clients. All registration messages between a visiting client and the home agent must contain the mobile-home authentication extension (MHAE). Proxy Mobile IP also implements this requirement in the registration messages sent by the access point on behalf of the visiting clients to the home agent.

The integrity of the registration messages is protected by a shared 128-bit key between the access point (on behalf of the visiting client) and the home agent. You can enter the shared key on the access point or on a RADIUS server.

The keyed message digest algorithm 5 (MD5) in prefix+suffix mode is used to compute the authenticator value in the appended MHAE. Mobile IP and proxy Mobile IP also support the hash-based message authentication code (HMAC-MD5). The receiver compares the authenticator value it computes over the message with the value in the extension to verify the authenticity.

Optionally, the mobile-foreign authentication extension and the foreign-home authentication extension are appended to protect message exchanges between a visiting client and foreign agent and between a foreign agent and home agent, respectively.

Replay protection uses the identification field in the registration messages as a timestamp and sequence number. The home agent returns its time stamp to synchronize the visiting client for registration. In proxy Mobile IP, the visiting clients are not synchronized to their home agents because the access point intercepts all home agent messages. If the timestamp in the first registration request is out of the tolerance window (± 7 seconds), the request is rejected. The access point uses the information from the rejection to create a valid value and resends the registration request.

The Proxy Mobile IP Setup Page

This section describes the Proxy Mobile IP Setup page and the links it provides to other pages you use to set up proxy Mobile IP on your access point. Figure 6-2 shows the Proxy Mobile IP Setup page.

Figure 6-2 Proxy Mobile IP Setup page



Follow this link path to reach the Proxy Mobile IP Setup page:

1. On the Summary Status page, click **Setup**.
2. In the Services section of the Setup page, click **Proxy Mobile IP**.

There are 5 links on the page:

- General
- Authentication Server
- Local SA Bindings
- Statistics
- View Subnet Map Table

General

Selecting the **General** link takes you to the Proxy Mobile IP General page (Figure 6-3), where you enable proxy Mobile IP on the access point and identify the IP addresses of the authoritative access points on your wireless network.

Figure 6-3 Proxy Mobile IP General Page

Settings on the Proxy Mobile IP General Page

Enable Proxy Mobile IP

This setting enables the proxy Mobile IP feature on the access point. The default setting is **no**.



Note

Proxy Mobile IP must also be enabled for the SSID you intend to use to support the feature. Otherwise, proxy Mobile IP will not work. See the “Configuring the Authoritative Access Point” section on page 6-21 for additional information.

Authoritative AP n

These settings identify the IP addresses of up to three authoritative access points (AAPs) on the wireless network. At least one AAP is required for the proxy Mobile IP enabled wireless network. The n represents the number of the authoritative access point. The authoritative access point is the device that registers with the home agent. After registering with the home agent, the AAP

populates a subnet map for other access points. The subnet map links the access points to the home agent to contact and register a mobile client based on the client's IP address. For example, if a mobile client appears with a "30" subnet IP address on the "20" subnet, the access point must register with the home agent that services subnet "30" mobile clients.

Authentication Server

Selecting the Authentication Server link takes you to the Authenticator Configuration page (Figure 6-4). From this page, you configure the RADIUS or TACACS servers that will be managing proxy Mobile IP wireless devices.

Figure 6-4 Authenticator Configuration Page

The screenshot shows the 'Authenticator Configuration Page' with a top bar containing 'Map' and 'Help' buttons, and a status indicator 'Uptime: 1 day, 19:55:08'. Below the top bar, there are two configuration fields: '802.1X Protocol Version (for EAP Authentication):' set to '802.1x-2001' and 'Primary Server Reattempt Period (Min.):' set to '0'. The main section is a table with columns: 'Server Name/IP', 'Server Type', 'Port', 'Shared Secret', 'Retran Int (sec)', and 'Max Retran'. There are four identical rows, each representing a server configuration. Each row has a text input for 'Server Name/IP', a dropdown for 'Server Type' (set to 'RADIUS'), a text input for 'Port' (set to '1812'), a masked text input for 'Shared Secret', a text input for 'Retran Int (sec)' (set to '5'), and a text input for 'Max Retran' (set to '3'). Below each row, there are four checkboxes: 'EAP Authentication' (checked), 'MAC Address Authentication' (unchecked), 'User Authentication' (unchecked), and 'MIP Authentication' (unchecked). At the bottom of the table, a note states: 'Note: For each authentication function, the most recently used server is shown in green text.' At the bottom right, there are four buttons: 'Apply', 'OK', 'Cancel', and 'Restore Defaults'.

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran
	RADIUS	1812		5	3
	RADIUS	1812		5	3
	RADIUS	1812		5	3
	RADIUS	1812		5	3

Use server for: ☒ EAP Authentication ☐ MAC Address Authentication ☐ User Authentication ☐ MIP Authentication

Note: For each authentication function, the most recently used server is shown in green text.

Apply OK Cancel Restore Defaults

Settings on the Authenticator Configuration Page

802.1X Protocol Version (for EAP Authentication)

This drop-down menu allows you to select the draft of the 802.1X protocol the access point's radio will use. EAP operates only when the radio firmware on client devices complies with the same 802.1X Protocol draft as the management firmware on the access point. See the “Setting Up EAP Authentication” section on page 8-20 for additional information.

Primary Server Reattempt Period (Min)

This field specifies how many minutes should pass before checking for the primary server when it was not initially accessible.

Server Name/IP

This field identifies the name or IP address of the RADIUS or TACACS server proxy Mobile IP is using for authentication purposes.

Server Type

This drop-down menu displays the selections you can make to designate the server type you want the proxy Mobile IP configuration to use. The choices are RADIUS or TACACS. RADIUS is the default setting.

Port

This field specifies the port number the server uses for authentication. The default setting, 1812, is the port setting for Cisco's RADIUS server, the Cisco Secure Access Control Server, and for many other RADIUS servers. Check your server's product documentation to find the correct port setting.

Shared Secret

This field identifies the shared secret used by your RADIUS server. The shared secret on the access point must match the shared secret on the RADIUS server. The shared secret can contain up to 64 alphanumeric characters. This setting has no default.

Retran Int (sec)

This field specifies the time interval in seconds that the server waits after it failed to contact the server until it tries again. The default setting is 5 seconds.

Max Retran

This field indicates how many times the server attempts to contact the server before it attempts to contact an alternate server. The setting works in conjunction with the Retran Int (sec) parameter.

Use server for:

These check boxes specify the authentication types the server uses: EAP, MAC Address, User, or MIP authentication. Checking the EAP authentication check box designates the server as an authenticator for any EAP type, including LEAP, PEAP, EAP-TLS, LEAP-SIM, and EAP-MD5.

Local SA Bindings

Selecting the Local SA Bindings link takes you to the Local SA Bindings page (Figure 6-5). You use this page to identify valid clients that are able to establish contact with a foreign agent in another network segment or network other than the client's home network.

Figure 6-5 Local SA Bindings Page

Home Map Network Associations Setup Logs Help 2002/11/26 03:13:55

New SA Binding:

IP Address Range - Start: Add

IP Address Range - End:

Group SPI:

Group Key:

Enter 32-bit SPI as 8 hexadecimal digits (0-9, a-f, or A-F) with range (100-FFFFFFF).
Enter 128-bit Key as 32 hexadecimal digits (0-9, a-f, or A-F).

Existing SA Bindings: Remove

10.30.0.20 10.30.0.25	100	14141414141414141414141414141414
10.30.0.26 10.30.0.27	100	14141414141414141414141414141414

Apply OK Cancel Restore Defaults 89657

Settings on the Local SA Bindings Page

IP Address Range - Start

This field contains the beginning IP address of the range in which client devices must reside in order to be valid.

IP Address Range - End

This field contains the ending IP address of the range in which the client devices must reside in order to be valid.

Group SPI

This field specifies the security parameter index of the IP address range entered in the IP Address Range - Start and End fields. The SPI is a 32-bit number (8 hexadecimal digits) assigned to the initiator of the security association request by the receiving IPsec endpoint. On receiving a packet, the destination address, protocol, and SPI are used to determine the security association. The security association allows the node to authenticate or decrypt the packet according to the security policy configured for that security association.

Group Key

This field contains an authentication key, similar to a WEP key, that the group specified in the security association uses to access a foreign agent. The group key is a 128-bit key entered as 32 hexadecimal digits (0-9, a-f, or A-F).

Existing SA Bindings

This field contains a listing of previously configured security association bindings. The information contains the beginning and ending IP address range and their associated group SPI and key settings.

Statistics

Selecting the Statistics link takes you to the Proxy Mobile IP Statistics page (Figure 6-6).

Two buttons are available on this page:

- **Refresh**—Click this button to refresh the data on the screen.
- **Clear**—Click this button to clear the data on the screen and begin a new round of data collection.

Figure 6-6 Proxy Mobile IP Statistics Page

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 3 days, 01:12:57
Mobile IP Status : Enabled Home Agents : Not found Foreign Agents : Not found Active AAP : 10.0.0.1 MIN IP Addresses :							
Solicitations Sent		119472	Registration Request Successes		0		
Authentication Failures for HA		0	Authentication Failures for FA		0		
Registration Requests Sent		0	Deregister Requests Sent		0		
Registration Replies Received		0	Deregister Replies Received		0		
Registration Requests Denied by FA		0	Registration Requests Denied by HA		0		
Advertisements Received		0	Gratuitous ARPs sent		0		

Settings on the Proxy Mobile IP Statistics Page

Mobile IP Status

This informational field indicates whether proxy Mobile IP is enabled or disabled.

Home Agents

This informational field provides information about home agents the access point discovers on its own subnet. If a home agent is discovered, its IP address is displayed. If no agent is discovered, the field displays Not Found.

Foreign Agents

This informational field provides information about foreign agents it discovers on the access point discovers on the network. If a foreign agent is discovered, its IP address is displayed. If multiple foreign agents are discovered, their IP addresses are displayed. If no agent is discovered, the field displays Not Found.

Active AAP

This informational field lists the IP address of the active authoritative access point. If multiple authoritative access points are configured, their IP addresses are displayed.

MN IP Addresses

This informational field lists the IP addresses of the mobile nodes, which are client devices that the access point is servicing.

Solicitations Sent

The number of agent solicitations messages the access point has sent. If the access point does not hear advertisements, it sends a solicitation message requesting a foreign or home agent acknowledgement. The solicitation forces any agents on the link to immediately send an agent advertisement.

Authentication Failures for HA

The number of times the home agent rejected registration requests because of authentication failures, such as an invalid SPI or group key. When a mobile node moves to a foreign network, the access point registers the mobile node to its home agent. This statistic indicates the number of registration failures caused by failure of the home agent or foreign agent to authenticate each other or the mobile node.

Registration Requests Sent

The number of registration requests sent by the access point for the mobile node.

Registration Request Denied by FA

The number of times a foreign agent rejected a registration request. When a mobile node moves to a foreign network, the access point registers the mobile node to its home agent. This statistic indicates the number of registration requests that were denied by the foreign agent. The reasons for denial vary and include home agent unreachable, no resources found, etc.

Advertisements Received

The number of IRDP advertisements received by agents.

Registration Requests Successes

The number of times registration requests were successful.

Authentication Failures for FA

The number of times the foreign agent rejected registration requests because of mobile node or home agent authentication failures.

Deregister Requests Sent

The number of times the access point sent deregistration requests to the home agent.

Deregister Replies Received

The number of times the access point received deregistration replies from the home agent.

Registration Requests Denied by HA

The number of times the home agent rejected registration requests.

Gratuitious ARPs sent

The number of times the access point sent gratuitious Address Resolution Protocol messages (ARPs). Gratuitious ARPs are sent by the home agent on behalf of a roaming mobile node to update the ARP caches on the local hosts. When the mobile node returns to its home network, the home access point sends gratuitious ARPs (on behalf of the mobile node) to notify the network of the mobile node’s MAC and IP address. In addition, the home agent also issues gratuitious ARPs for the mobile node in case there are nodes who could not hear the mobile node.

View Subnet Map Table

Selecting the View Subnet Map Table link takes you to the Subnet Map Table page (Figure 6-7). The subnet map table contains a list of home agent IP addresses and their associated subnet masks.

Two buttons are available on this page that are not shown on Figure 6-7:

- Clear—removes entries that are no longer valid
- Refresh—validates and renews entries on the table

Figure 6-7 Subnet Map Table Page

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 00:30:19
HA Address		Subnet Mask					
10.30.0.1		255.255.255.0					
10.20.0.1		255.255.255.0					

Settings on the Subnet Map Table Page

HA Address

This column lists the IP addresses of the home agents.

Subnet Mask

This column lists the subnet mask addresses for the corresponding home agents.

Configuring Proxy Mobile IP

Proxy Mobile IP functions as a proxy on behalf of roaming clients that do not implement a Mobile IP software stack. In a Mobile IP environment, the access point uses the services of a home agent and a foreign agent to allow valid mobile nodes to access a working Mobile IP network on a wired LAN. A working Mobile IP network assumes the following:

- At least one router in the network functions as a home agent where mobile clients will be based.
- At least one router in the network functions as a foreign agent, to which mobile clients will roam.
- Access points configured as authoritative access points must be enabled for proxy Mobile IP before regular access points.
- All proxy Mobile IP enabled access points in the network must be configured to use the same authoritative access points. For example, one access point cannot be configured with two authoritative access points and another access point be configured with three different authoritative access points.

Optionally, you can implement an AAA server to authenticate mobile clients in addition to home and foreign agents.

Before You Begin

Before configuring proxy Mobile IP, you should consider these guidelines:

- You can enable proxy Mobile IP only on root access points (units connected to the wired LAN). You cannot enable proxy Mobile IP on repeater access points or bridges.
- Access points participating in proxy Mobile IP should be configured with gateway addresses. You can configure the gateways manually, or the access points can receive gateways through DHCP.
- The foreign and home agents must reside on the network gateways where you want to support proxy Mobile IP.
- If your authoritative access points receive their IP addresses through DHCP, use the access point host names to specify the AAPs in the proxy Mobile IP configuration.
- Proxy Mobile IP does not support broadcast and multicast traffic for visiting clients.
- To use proxy Mobile IP with DHCP-enabled client devices, you must disable Media Sense on the client devices. You can find instructions for disabling Media Sense in *Microsoft Knowledge Base Article Q239924*. Click this URL to browse to this article:
<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q239924>
- Proxy Mobile IP does not support VLANs.

Configuring Proxy Mobile IP on Your Wired LAN

Proxy Mobile IP on access points works in conjunction with Mobile IP configured on your network routers. For instructions on configuring Mobile IP on a router on your network, refer to the Mobile IP chapter in *12.2 T New Features (Early Deployment Releases)*. Click this link to browse to the Mobile IP chapter:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/mobileip.htm>

In addition, make sure you have accomplished the following items:

- Loaded the latest firmware onto all access points in your wireless network.
- Established an HTTP connection to the access point.

- Verified that client devices are associated to the local access point.
- Verified receipt of an appropriate DHCP address for the local LAN segment.
- Confirmed IP connectivity between all devices (ping or HTTP).

Configuring the Authoritative Access Point

Proxy Mobile IP must be enabled on the wireless SSID. Since multiple SSIDs may exist on the access point and not all SSIDs may have to accommodate mobile clients, you must enable proxy Mobile IP per SSID. The AAP is used to communicate with new access points to update subnet map records and send the new access points a new and complete subnet mapping table. The AAP also contacts all the other access points listed in the table and sends update packets containing the changed information. In this way the other access points update their subnet mapping tables. For example, if a mobile device appears with a “30” subnet IP address on the “20” subnet, the access point must register the client with the home agent that services the mobile clients on the “30” subnet.

Follow these steps to configure the authoritative access point.

-
- Step 1** Browse to the access point’s Setup page.
 - Step 2** In the Associations section, click **SSIDs: Int**. The AP Radio: Internal Service Sets page appears.
 - Step 3** Select the SSID you intend to use by mobile clients and click **Edit**. The AP Radio: Internal SSID #x page appears (Figure 6-8).

Figure 6-8 AP Radio Internal SSID #x Page

Uptime: 4 days, 01:38:36

Map Help

Device: AP Radio: Internal

Service Set ID (SSID): bnetwork30

Current Number of Associations: 0

Maximum Number of Associations: 0

Proxy Mobile IP is enabled: ☒ yes ☐ no

Default VLAN ID: [0] -None-

Default Policy Group ID: [0] -None-

Accept Authentication Type: ☒ Open ☐ Shared ☐ Network-EAP

Require EAP: ☐

Default Unicast Address Filter: Allowed Allowed Allowed

To require static or server-based MAC-Address authentication, set "Default Unicast Address Filter" to "Disallowed".

Apply OK Cancel Restore Defaults

- Step 4** Set the Proxy Mobile IP setting to **yes**.
- Step 5** Click **OK**. You are returned to the AP Radio: Internal Service Sets page.
- Step 6** Click **OK** again. You are returned to the Setup page.
- Step 7** In the Services section, click **Proxy Mobile IP**. The Proxy Mobile IP Setup page appears (Figure 6-9).

Figure 6-9 Proxy Mobile IP Setup Page

Home Map Network Associations Setup Logs Help

Uptime: 00:19:57

[General](#)

[Authentication Server](#)

[Local SA Bindings](#)

[Statistics](#)

[View Subnet Map Table](#)

Done

- Step 8** Click **General**. The Proxy Mobile IP General page appears (Figure 6-10).

Figure 6-10 Proxy Mobile IP General Page

- Step 9** Set the Enable Proxy Mobile IP setting to **yes**.
- Step 10** Enter the IP address of the access point in the Authoritative AP 1 field.
- Step 11** Click **OK**. You are returned to the Proxy Mobile IP Setup page.
- Step 12** Click **View Subnet Map Table**. The Subnet Map Table appears (Figure 6-11).

Figure 6-11 Subnet Map Table

HA Address	Subnet Mask
10.30.0.1	255.255.255.0
10.20.0.1	255.255.255.0

- Step 13** Check the IP addresses in the HA Address column. The home agent’s IP address should appear in this column.

Configuring the Access Point on a Home or Foreign Network

At least one access point on the wireless side of a home and foreign network must be a home or foreign agent access point. Both access points must be configured to enable valid mobile nodes to associate with them and be detected by the authoritative access point.

There are no “standard” procedures that describe how to configure these agent access points. Configuration parameters, such as SSIDs, valid proxy Mobile IP addresses, SPI keys and group keys, and security settings must be carefully considered and coordinated with wired side router settings before any degree of success can be expected. The basic settings are the same for both access points. The only difference is where the access point is located. A home agent access point is on the wireless side of the mobile node’s home network. A foreign agent access point is on the wireless side of the network the mobile node is authorized to enter in order to communicate back to its home network.

These instructions provide a general overview of the steps involved to configure the wireless network components to operate in a mobile IP environment. It must be stressed that the majority of configuration effort is devoted to components on the wired network.

Follow these steps to configure a home or foreign agent access point.

-
- Step 1** Configure the access point normally (SSID, security, etc.).
 - Step 2** From the Associations section of the Setup page, select the SSID for the radio you are configuring. The Service Set Summary Status page appears.
 - Step 3** Highlight the SSID you are using for the mobile nodes and click **Edit**. The AP Radio Internal SSID #*n* appears.
 - Step 4** Set the Proxy Mobile IP is enabled radio button to **yes** and click **OK** to return to the Service Set Summary Status page.
 - Step 5** Click **OK** again to return to the Setup page.
 - Step 6** In the Services section of the Setup page, click **Proxy Mobile IP**. The Proxy Mobile IP Setup page appears.
 - Step 7** Click **General**. The Proxy Mobile IP General page appears.
 - Step 8** Set the Enable Proxy Mobile IP radio button to **yes**.
 - Step 9** Enter the IP address of the authoritative access point in the Authoritative AP 1: field.
 - Step 10** Click **OK** to return to the Proxy Mobile IP Setup page.
 - Step 11** Click **Local SA Bindings**. The Local SA Bindings page appears.
 - Step 12** Enter the starting and ending IP addresses of the range of IP addresses designated as valid mobile node addresses.
 - Step 13** Enter a predetermined SPI and Group Key in the appropriate fields.

Step 14 Click **OK** to return to the Proxy Mobile IP Setup page.

Step 15 Click **Done** to return to the Setup page.



Configuring Other Settings

This chapter identifies and provides information on how to configure other settings on the access point, such as servers and association tables.

This chapter contains the following sections:

- Server Setup, page 7-2
- Routing Setup, page 7-11
- Association Table Display Setup, page 7-13
- Event Notification Setup, page 7-18

Server Setup

This section describes how to configure the server to support access point features. You use separate management system pages to enter server settings. The server setup pages are described in the following sections:

- Entering Time Server Settings, page 7-2
- Entering Boot Server Settings, page 7-4
- Entering Web Server Settings and Setting Up Access Point Help, page 7-7
- Entering Name Server Settings, page 7-9

**Note**

See the “Enabling EAP on the Access Point” section on page 8-20 for instructions on setting up the authentication server.

Entering Time Server Settings

You use the Time Server Setup page to enter time server settings. Figure 7-1 shows the Time Server Setup page:

Figure 7-1 Time Server Setup Page

Follow this link path to reach the Time Server Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Time Server** under Services.

Settings on the Time Server Setup Page

The Time Server Setup page contains the following settings:

- Simple Network Time Protocol
- Default Time Server
- GMT Offset (hr)
- Use Daylight Savings Time
- Manually Set Date and Time

The page also shows the active time server.

Simple Network Time Protocol

Select **Enabled** or **Disabled** to turn Simple Network Time Protocol (SNTP) on or off. If your network uses SNTP, select **Enabled**.

Default Time Server

If your network has a default time server, enter the server's IP address in the Default Time Server entry field.

The Current Time Server line under the entry field reports the time server the access point is currently using.

**Note**

The DHCP or BOOTP server can override the default time server.

GMT Offset (hr)

The GMT Offset drop-down menu lists the world's time zones relative to Greenwich Mean Time (GMT). Select the time zone in which the access point operates.

Use Daylight Savings Time

Select **yes** or **no** to have the access point automatically adjust to Daylight Savings Time.

Manually Set Date and Time

Enter the current date and time in the entry fields to override the time server or to set the date and time if no server is available.

When entering the date and time, use forward-slashes to separate the year, month, and day, and use colons to separate the hours, minutes, and seconds. For example, you would enter 2001/02/17 for February 17, 2001, and 18:25:00 for 6:25 pm.

Entering Boot Server Settings

You use the Boot Server Setup page to configure the access point for your network's BOOTP or DHCP servers for automatic assignment of IP addresses. Figure 7-2 shows the Boot Server Setup page:

Figure 7-2 Boot Server Setup Page

The screenshot shows the 'Boot Server Setup' page with the following fields and controls:

- Map** and **Help** buttons at the top left.
- Uptime:** 6 days, 21:54:44 at the top right.
- Configuration Server Protocol:** A dropdown menu set to **DHCP**.
- Use previous Configuration Server settings when no server responds?** Radio buttons for **yes** (selected) and **no**.
- Read ".ini" file from file server?** A dropdown menu set to **if specified by server**, with a **Load Now** button below it.
- Current Boot Server:** 0.0.0.0
- Specified ".ini" File Server:** 0.0.0.0
- BOOTP Server Timeout (sec):** 120
- DHCP Multiple-Offer Timeout (sec):** 5
- DHCP Requested Lease Duration (min):** 1440
- DHCP Minimum Lease Duration (min):** 0
- DHCP Client Identifier Type:** Ethernet (10Mb)
- DHCP Client Identifier Value:** 004096406fe6
- DHCP Class Identifier:** AP4800E
- At the bottom right, there are buttons for **Apply**, **OK**, **Cancel**, and **Restore Defaults**.

Follow this link path to reach the Boot Server Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Boot Server** under Services.

Settings on the Boot Server Setup Page

The Boot Server Setup page contains the following settings:

- Configuration Server Protocol
- Use Previous Configuration Server Settings
- Read .ini File from File Server
- BOOTP Server Timeout (sec)
- DHCP Multiple-Offer Timeout (sec)
- DHCP Requested Lease Duration (min)
- DHCP Minimum Lease Duration (min)
- DHCP Client Identifier Type
- DHCP Client Identifier Value
- DHCP Class Identifier

The page also shows the IP address of the current boot server and specified “.ini” file server.

Configuration Server Protocol

Use the Configuration Server Protocol drop-down menu to select your network's method of IP address assignment. The menu contains the following options:

- None—Your network does not have an automatic system for IP address assignment.
- BOOTP—Your network uses Boot Protocol, in which IP addresses are hard-coded based on MAC addresses.
- DHCP—With Dynamic Host Configuration Protocol, IP addresses are leased for a period of time. You can set the lease duration with the settings on this page.

Use Previous Configuration Server Settings

Select **yes** to have the access point save the boot server's most recent response. The access point uses the most recent settings if the boot server is unavailable.

Read .ini File from File Server

Use this setting to have the access point use configuration settings in an .ini file on the BOOTP or DHCP server or the default file server. Files with .ini extensions usually contain configuration information used during system start-up. The drop-down menu contains the following options:

- Always—The access point always loads configuration settings from an .ini file on the server.
- Never—The access point never loads configuration settings from an .ini file on the server.
- If specified by server—The access point loads configuration settings from an .ini file on the server if the server's DHCP or BOOTP response specifies that an .ini file is available. This is the default setting.

The Load Now button under the drop-down menu tells the access point to read an .ini file immediately.

The Current Boot Server line under the drop-down menu lists the server that responded to the access point's boot request. If all zeros appear, it means that the access point is not using BOOTP/DHCP or that no server responded to the BOOTP/DHCP request. The Specified ".ini" File Server line lists the IP address of the server where the .ini file is stored. If all zeroes appear, it means that no file server is set up to provide an .ini file.

BOOTP Server Timeout (sec)

This setting specifies the length of time the access point waits to receive a response from a single BOOTP server. Enter the number of seconds the access point should wait. This setting applies only when you select BOOTP from the Configuration Server Protocol drop-down menu.

DHCP Multiple-Offer Timeout (sec)

This setting specifies the length of time the access point waits to receive a response when there are multiple DHCP servers. Enter the number of seconds the access point should wait.

DHCP Requested Lease Duration (min)

This setting specifies the length of time the access point requests for an IP address lease from your DHCP server. Enter the number of minutes the access point should request.

DHCP Minimum Lease Duration (min)

This setting specifies the shortest amount of time the access point accepts for an IP address lease. The access point ignores leases shorter than this period. Enter the minimum number of minutes the access point should accept for a lease period.

DHCP Client Identifier Type

Use this optional setting to include a class identifier type in the DHCP request packets the access point sends to your DHCP server. Your DHCP server can be set up to send responses according to class identifier type. If most of the client devices using the access point are the same device type, you can select that device type to be included in the DHCP request packet.

Use **Ethernet (10Mb)**, the default setting, if you do not intend to set up your DHCP server to send responses according to class identifier type.

If you want to include a unique value in the DHCP Client Identifier Value field (the setting under DHCP Client Identifier Type on the Boot Server Setup page), select **Other - Non Hardware**.

Table 7-1 lists the options in the DHCP Client Identifier Type drop-down menu.

Table 7-1 Options in the DHCP Client Identifier Type Menu

Option	Definition
Ethernet (10Mb)	This is the default setting. Use this setting if you do not need your DHCP server to send responses based on the class identifier in the access point's DHCP request packets.
Experimental Ethernet	Select one of these specific device types if most of the client devices using the access point are the same device type. The access point includes the device type in the DHCP request packets it sends to the DHCP server.
Amateur Radio AX.25	
Proteon ProNET Token Ring	
Chaos	
IEEE 802 Networks	
ARCNET	
Hyperchannel	
Lanstar	
Autonet Short Address	
LocalTalk	
LocalNet	
Other - Non Hardware	Select this option to include a unique value in the DHCP Client Identifier Value field.

DHCP Client Identifier Value

Use this setting to include a unique identifier in the access point's DHCP request packet. This field contains the access point's MAC address by default. If you select **Other - Non Hardware** from the DHCP Client Identifier Type drop-down menu, you can enter up to 255 alphanumeric characters. If you select any other option from the DHCP Client Identifier Type drop-down menu, you can enter up to 12 hexadecimal characters. Hexadecimal characters include the numbers 0 through 9 and the letters A through F.

DHCP Class Identifier

Your DHCP server can be set up to send responses according to the group to which a device belongs. Use this field to enter the access point's group name. The DHCP server uses the group name to determine the response to send to the access point. The access point's DHCP class identifier is a vendor class identifier.

Entering Web Server Settings and Setting Up Access Point Help

You use the Web Server Setup page to enable browsing to the web-based management system, specify the location of the access point Help files, and enter settings for a custom-tailored web system for access point management. Figure 7-3 shows the Web Server Setup page:

Figure 7-3 Web Server Setup Page

The screenshot shows the 'Web Server Setup' page with a yellow background. At the top left are 'Map' and 'Help' links. At the top right is the 'Uptime: 02:30:58' status. The main configuration area includes:

- 'Allow Non-Console Browsing?' with radio buttons for 'yes' (selected) and 'no'.
- 'HTTP Port:' with a text box containing '80'.
- 'Default Help Root URL:' with a text box containing 'file:///C:/Cisco/Help'.
- 'Extra Web Page File:' with an empty text box and a 'Load Now' button to its right.
- 'Default Web Root URL:' with a text box containing 'mfs0:/StdUI/'.

 At the bottom are four buttons: 'Apply', 'OK', 'Cancel', and 'Restore Defaults'. A vertical label '409336' is on the right side of the form area.

Follow this link path to reach the Web Server Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Web Server** under Services.

Settings on the Web Server Setup Page

The Web Server Setup page contains the following settings:

- Allow Non-Console Browsing
- HTTP Port
- Default Help Root URL
- Extra Web Page File
- Default Web Root URL

Allow Non-Console Browsing

Select **yes** to allow browsing to the management system. If you select no, the management system is accessible only through the console and Telnet interfaces.

HTTP Port

This setting determines the port through which your access point provides web access. Your System Administrator should be able to recommend a port setting.

Default Help Root URL

This entry tells the access point where to look for the Help files. The Help button on each management system page opens a new browser window displaying help for that page. The online help files are provided on the access point and bridge CD in the Help directory. You can point to the help files in one of four possible locations:

- Internet—Cisco maintains up-to-date help for access points on the Cisco website. While this location requires online access for every occasion of needing online help, it offers the most up-to-date information. If you use this help location, which is the default setting, you don't need to copy the files from the access point and bridge CD.
- File Server—On multi-user networks, the help files can be placed on the network file server. For this location, enter the full directory URL in the Default Help Root URL entry field. Your entry might look like this:
`[system name]\[directory]\wireless\help`
- Hard Drive—you can copy the help files to the hard drive of the computer you use to manage the wireless LAN. If you use this location, enter the full directory URL. Your entry might look like this:
`file:/// [drive letter]:\[folder or subdirectory]\wireless\help`

Extra Web Page File

If you need to create an alternative to the access point's management system, you can create HTML pages and load them into the access point. You use this entry field to specify the filename for your HTML page stored on the file server.

Click **Load Now** to load the HTML page.

Default Web Root URL

This setting points to the access point management system's HTML pages. If you create alternative HTML pages, you should change this setting to point to the alternative pages. The default setting is: mfs0:/StdUI/

Entering Name Server Settings

You use the Name Server Setup page to configure the access point to work with your network's Domain Name System (DNS) server. Figure 7-4 shows the Name Server Setup page:

Figure 7-4 The Name Server Setup Page

The screenshot shows the 'Name Server Setup' page with a yellow background. At the top left are 'Map' and 'Help' buttons. At the top right is the 'Uptime: 02:32:22' status. The main configuration area includes:

- Domain Name System (DNS):** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Default Domain:** A text box containing 'company.com'.
- Current Domain:** A text box containing 'company.com'.
- Domain Name Servers:** A table with two columns: 'Default' and 'Current'.

	Default	Current
1.	209.165.200.229	209.165.200.229
2.	209.165.200.240	209.165.200.240
3.		
- Domain Suffix:** A text box containing '.company.com'.

At the bottom right are four buttons: 'Apply', 'OK', 'Cancel', and 'Restore Defaults'. A small '409090' icon is visible on the far right edge.

Follow this link path to reach the Name Server Setup page:

- On the Summary Status page, click **Setup**
- On the Setup page, click **Name Server** under Services.

Settings on the Name Server Setup Page

The Name Server Setup page contains the following settings:

- Domain Name System
- Default Domain
- Domain Name Servers
- Domain Suffix

Domain Name System

If your network uses a Domain Name System (DNS), select **Enabled** to direct the access point to use the system. If your network does not use DNS, select **Disabled**.

Default Domain

Enter the name of your network's IP domain in the entry field. Your entry might look like this:

mycompany.com

The Current Domain line under the entry field lists the domain that is serving the access point. The current domain might be different from the domain in the entry field if, on the Boot Server Setup page, you have DHCP or BOOTP set as the Configuration Server Protocol, but you selected No for the setting “Use previous Configuration Server settings when no server responds?”

Domain Name Servers

Enter the IP addresses of up to three domain name servers on your network. The Current lines to the right of the entry fields list the servers the access point is currently using, which may be specified by the DHCP or BOOTP server.

Domain Suffix

In this entry field, enter the portion of the full domain name that you would like omitted from access point displays. For example, in the domain “mycompany.com” the full name of a computer might be “mycomputer.mycompany.com.” With domain suffix set to “mycompany.com,” the computer's name would be displayed on management system pages as simply “mycomputer.”

Entering FTP Settings

You use the FTP Setup page to assign File Transfer Protocol settings for the access point. All non-browser file transfers are governed by the settings on this page. Figure 7-5 shows the FTP Setup page:

Figure 7-5 The FTP Setup Page

The screenshot shows the FTP Setup page with a yellow background. At the top left are links for [Map](#) and [Help](#). At the top right is the text "Uptime: 02:37:33". The main area contains five labeled fields: "File Transfer Protocol:" with a dropdown menu showing "FTP"; "Default File Server:" with an empty text box; "FTP Directory:" with an empty text box; "FTP User Name:" with a text box containing "anonymous"; and "FTP User Password:" with a text box containing "*****". At the bottom right are four buttons: "Apply", "OK", "Cancel", and "Restore Defaults". A vertical text "40918" is visible on the right edge of the form area.

Follow this link path to reach the FTP Setup page:

- On the Summary Status page, click **Setup**
- On the Setup page, click **FTP** under Services.

Settings on the FTP Setup Page

The FTP Setup page contains the following settings:

- File Transfer Protocol
- Default File Server
- FTP Directory
- FTP User Name
- FTP User Password

File Transfer Protocol

Use the drop-down menu to select **FTP** or **TFTP** (Trivial File Transfer Protocol). TFTP is a relatively slow, low-security protocol that requires no username or password.

Default File Server

Enter the IP address or DNS name of the file server where the access point should look for FTP files.

FTP Directory

Enter the file server directory that contains the firmware image files.

FTP User Name

Enter the username assigned to your FTP server. You don't need to enter a name in this field if you select TFTP as the file transfer protocol.

FTP User Password

Enter the password associated with the file server's username. You don't need to enter a password in this field if you select TFTP as the file transfer protocol.

Routing Setup

You use the Routing Setup page to configure the access point to communicate with the IP network routing system. You use the page settings to specify the default gateway and to build a list of installed network route settings. Figure 7-6 shows the Routing Setup page.

Figure 7-6 Routing Setup Page

The screenshot shows the 'Routing Setup' page with a yellow background. At the top left are 'Map' and 'Help' buttons. At the top right is the 'Uptime: 02:38:32' status. The main section contains three primary areas: 'Default Gateway' with a text field containing '209.165.200.201'; 'New Network Route' with three stacked text fields for 'Dest Network:', 'Gateway:', and 'Subnet Mask:', followed by an 'Add' button; and 'Installed Network Routes' with a scrollable list box and a 'Remove' button. At the bottom are four buttons: 'Apply', 'OK', 'Cancel', and 'Restore Defaults'. A small vertical number '40924' is visible on the right edge.

Follow this link path to reach the Routing Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Routing** under Services.

Entering Routing Settings

The Routing Setup page contains the following settings:

- Default Gateway
- New Network Route Settings
- Installed Network Routes List

Default Gateway

Enter the IP address of your network's default gateway in this entry field. The entry 255.255.255.255 indicates no gateway.

New Network Route Settings

You can define additional network routes for the access point. To add a route to the installed list, fill in the three entry fields and click **Add**. To remove a route from the list, highlight the route and click **Remove**. The three entry fields include:

- Dest Network—Enter the IP address of the destination network.
- Gateway—Enter the IP address of the gateway used to reach the destination network.
- Subnet Mask—Enter the subnet mask associated with the destination network.

Installed Network Routes List

The list of installed routes provides the destination network IP address, the gateway, and the subnet mask for each installed route.

Association Table Display Setup

You use the Association Table Filters and the Association Table Advanced pages to customize the display of information in the access point's Association Table.

Association Table Filters Page

Figure 7-7 shows the Association Table Filters page.

Figure 7-7 Association Table Filters Page

Map Help Uptime: 02:39:47

Stations to Show: ☒ Client ☒ Repeater ☒ Bridge ☒ AP
☐ Infra. Host ☐ Multicast ☐ Entire Network

Fields to Show: ☒ System Name ☒ IP Address ☒ Device ☐ Class
☒ State ☒ Parent ☐ SW Version ☐ Total ☐ Alert

Packets To/From Station: ☐ Total ☐ Alert
Bytes To/From Station: ☐ Total ☐ Alert

Primary Sort: ☒ Device ☐ System Name ☐ IP Addr./Name ☐ MAC Address ☐ Class ☐ Parent
Secondary Sort: ☐ Device ☒ System Name ☐ IP Addr./Name ☐ MAC Address ☐ Class

OK Cancel Restore Defaults 43003

Follow this link path to reach the Association Table Filters page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Display Defaults** under Associations.

You can also reach the Association Table Filters page through the “additional display filters” link on the Association Table page. When you reach the page through the “additional display filters” link, four buttons appear at the bottom of the page that are different from the standard buttons on management system pages. The buttons include:

- **Apply**—Applies your selections to the Association Table and returns you to the Association Table page.
- **Save as Default**—Saves your selections as new default settings and returns you to the Association Table page.

- **Restore Current Defaults**—Applies the currently saved default settings to the Association Table and returns you to the Association Table page.
- **Restore Factory Defaults**—Applies the factory default settings to the Association Table and returns you to the Association Table page.

Settings on the Association Table Filters Page

The Association Table Filters page contains the following settings:

- Stations to Show
- Fields to Show
- Packets To/From Station
- Bytes To/From Station
- Primary Sort
- Secondary Sort

Stations to Show

Select the station types that you want to be displayed in the Association Table. If you select all station types, all stations of these types appear in the access point's Association Table.

Fields to Show

The fields you select here are the column headings for the Association Table. Fields include:

- **System Name**—A device's system name.
- **State**—A device's operational state. Possible states include:
 - **Assoc**—The station is associated with an access point.
 - **Unauth**—The station is unauthenticated with any access point.
 - **Auth**—The station is authenticated with an access point.
- **IP Address**—A device's IP address.
- **Parent**—A wireless client device's parent device, which is usually an access point.
- **Device**—A device's type, such as a 350 series access point or a PC Client Card. Non-Aironet devices appear as "Generic 802.11" devices.
- **SW Version**—The current version of firmware on a device.
- **Class**—A device's role in the wireless LAN. Classes include:
 - **AP**—an access point station.
 - **Client or PS Client**—a client or power-save client station.
 - **Bridge, Bridge R**—a bridge or a root bridge.
 - **Rptr**—a repeater access point.
 - **Mcast**—a multicast address.
 - **Infra**—an infrastructure node, usually a workstation with a wired connection to the Ethernet network.

Packets To/From Station

Use these settings to display packet volume information in the Association Table. Select **Total** to display the total number of packets to and from each station on the network.

Select **Alert** to display the number of alert packets to and from each station on the network for which you have activated alert monitoring. Select the **Alert** checkbox on a device's Station page to activate alert monitoring for that device. See the "Using Station Pages" section on page 9-3 for details on Station pages.

The Total and Alert selections both add a column to the Association Table.

Bytes To/From Station

Use these settings to display byte volume information in the Association Table. Select **Total** to display the total number of bytes to and from each station on your wireless network. Select **Alert** to display the number of alert bytes to and from each station on the wireless network. Both selections add a column to the Association Table.

Primary Sort

This setting determines the information that appears in the first column in the Association Table.

Secondary Sort

This setting determines the information that appears in the second column in the Association Table.

Association Table Advanced Page

You use the Association Table Advanced page to control the total number of devices the access point can list in the Association Table and the amount of time the access point continues to track each device class when a device is inactive. Figure 7-8 shows the Association Table Advanced page.

Figure 7-8 Association Table Advanced Page

Map Help Uptime: 3 days, 20:26:49

Handle Alerts as Severity Level External Information

Maximum number of bytes stored per Alert packet 0

Maximum Number of Forwarding Table Entries: 8192

Rogue AP Alert Timeout (minutes) 30

Aironet Extended Statistics in MIB (awcTpFdbTable): ☒ Enabled ☐ Disabled

Block ALL Inter-Client Communications ("PSPF"): ☐ Yes ☒ No

Default Activity Timeout (seconds) Per Device Class:

Unknown Class	300
Multicast Addresses	28800
Infrastructure Hosts	1800
Client Stations	1800
Repeaters	28800
Access Points	28800
Across-Bridge Hosts	1800
Non-Root Bridges	28800
Root Bridges	28800

Apply OK Cancel Restore Defaults

81744

Follow this link path to reach the Association Table Advanced page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Advanced** under Associations.

Settings on the Association Table Advanced Page

The Association Table Advanced page contains the following settings:

- Handle Station Alerts as Severity Level
- Maximum number of bytes stored per Station Alert packet
- Maximum Number of Forwarding Table Entries
- Rogue AP Alert Timeout (minutes)
- Aironet Extended Statistics in MIB (awcTpFdbTable)
- Block ALL Inter-Client Communications (PSPF)
- Default Activity Timeout (seconds) Per Device Class

Handle Station Alerts as Severity Level

This setting determines the Severity Level at which Station Alerts are reported in the Event Log. This setting also appears on the Event Handling Setup page. You can choose from four Severity Levels:

- Fatal Severity Level (System, Protocol, Port)—Fatal-level events indicate an event that prevents operation of the port or device. For operation to resume, the port or device usually must be reset. Fatal-level events appear in red in the Event Log.
- Alert Severity Level (System, Protocol, Port, External)—Alert-level messages indicate that you need to take action to correct the condition and appear in magenta in the Event Log.
- Warning Severity Level (System, Protocol, Port, External)—Warning-level messages indicate that an error or failure may have occurred and appear in blue in the Event Log.
- Information Severity Level (System, Protocol, Port, External)—Information-level messages notify you of some sort of event, not fatal (that is, the port has been turned off, the rate setting has been changed, etc.) and appear in green in the Event Log.

Maximum number of bytes stored per Station Alert packet

This setting determines the maximum number of bytes the access point stores for each Station Alert packet when packet tracing is enabled. If you use 0 (the default setting), the access point does not store bytes for Station Alert packets; it only logs the event. See the “Event Handling Setup Page” section on page 7-21 for instructions on enabling packet tracing.

Maximum Number of Forwarding Table Entries

This setting determines the maximum number of devices that can appear in the Association Table.

Rogue AP Alert Timeout (minutes)

When an access point detects a rogue access point, it sends an alert message to the system log. This setting specifies the amount of time in minutes the access point transmits the alert message. When the timeout is reached, the access point stops sending the alert message.

Aironet Extended Statistics in MIB (awcTpFdbTable)

Use this setting to enable or disable the storage of detailed statistics in access point memory. When you disable extended statistics you conserve memory, and the access point can include more devices in the Association Table.

Block ALL Inter-Client Communications (PSPF)

Publicly Secure Packet Forwarding (PSPF) prevents client devices associated to an access point from inadvertently sharing files with other client devices on the wireless network. It provides Internet access to client devices without providing other capabilities of a LAN. With PSPF enabled, client devices cannot communicate with other client devices on the wireless network. This feature is useful for public wireless networks like those installed in airports or on college campuses.



Note

The PSPF feature is available in firmware versions 11.08 and later, which are available on Cisco.com. You can download Cisco Aironet firmware releases at <http://www.cisco.com/public/sw-center/sw-wireless.shtml>.

Default Activity Timeout (seconds) Per Device Class

These settings determine the number of seconds the access point continues to track an inactive device depending on its class. A setting of zero tells the access point to track a device indefinitely no matter how long it is inactive. A setting of 300 equals 5 minutes; 1800 equals 30 minutes; 28800 equals 8 hours.

Event Notification Setup

You use the Event Display Setup, Event Handling Setup, and Event Notifications Setup pages to customize the display of access point events (alerts, warnings, and normal activity).

Event Display Setup Page

You use the Event Display Setup page to determine how time should be displayed on the Event Log. In addition, you can determine what severity level is significant enough to display an event. Figure 7-9 shows the Event Display Setup page.

Figure 7-9 The Event Display Setup Page

Map Help Uptime: 02:45:33

How should time generally be displayed? Wall-Clock Time

How should Event Elapsed (non-wall-clock) Time be displayed? Since Boot

Severity Level at which to display events immediately on the console: External Information

Severity Level at which to display events on the console log: External Information

Severity Level at which to display events on the GUI log: External Information

Apply OK Cancel Restore Defaults 49012

Follow this link path to reach the Event Display Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Display Defaults** under Event Log.

Settings on the Event Display Setup Page

The Event Display Setup page contains the following settings:

- How should time generally be displayed?
- How should Event Elapsed (non-wall-clock) Time be displayed?
- Severity Level at which to display events

How should time generally be displayed?

You use this drop-down menu to determine whether the events in the Event Log are displayed as system uptime or wall-clock time. If you select system uptime, the events are displayed either since the boot or since the last time the Event Log was displayed. If you select wall-clock time, the events are displayed in a YY:MM:DD HH:MM:SS format. If time has not been set on the access point (either manually or by a time server), the time display appears as uptime regardless of this selection.

How should Event Elapsed (non-wall-clock) Time be displayed?

Choose to display event time since the last boot-up of the access point or the time that has elapsed since the event occurred.

Severity Level at which to display events

When an event occurs, it may be displayed immediately on the console, on the console log, or on the GUI log for read purposes only. The event may also be recorded. (You control display and recording of events through the Event Handling Setup page; see the “Event Handling Setup Page” section on page 7-21 for details.) Use the drop-down menus to choose one of the sixteen severity levels for each display area. Table 7-2 lists the severity levels.

Table 7-2 Event Display Severity Levels

Severity Level	Description
silent	The *silent* setting directs the access point to not display any events immediately on the console, the console log, or the GUI log.
System Fatal Protocol Fatal Port Fatal	<p>The Fatal settings indicate an event that prevents operation of the port or device. For operation to resume, the port or device usually must be reset.</p> <ul style="list-style-type: none"> • System refers to the access point as a whole. • Protocol refers to a specific communications protocol in use, such as HTTP or IP. • Port refers to the access point’s Ethernet or radio network interface.
System alert Protocol alert Port alert External alert	<p>The Alert settings indicate events of which an administrator specifically requested to be informed.</p> <ul style="list-style-type: none"> • System refers to the access point as a whole. • Protocol refers to a specific communications protocol in use, such as HTTP or IP. • Port refers to the access point’s Ethernet or radio network interface. • External refers to a device on the network other than the access point.

Table 7-2 Event Display Severity Levels (continued)

Severity Level	Description
System warning Protocol warning Port warning External warning	<p>The Warning settings indicate that a failure has occurred.</p> <ul style="list-style-type: none">• System refers to the access point as a whole.• Protocol refers to a specific communications protocol in use, such as HTTP or IP.• Port refers to the access point's Ethernet or radio network interface.• External refers to a device on the network other than the access point.
System information Protocol information Port information External information	<p>The Information settings indicate a normal action that isn't fatal (that is, the port has been turned off, the rate setting has been changed, etc.)</p> <ul style="list-style-type: none">• System refers to the access point as a whole.• Protocol refers to a specific communications protocol in use, such as HTTP or IP.• Port refers to the access point's Ethernet or radio network interface.• External refers to a device on the network other than the access point.

These selections affect display of events only. They are used to filter information, not to remove it from the Event Log. To remove information from the Event Log, click **Purge Log** on the Event Log page.

Event Handling Setup Page

You use the Event Handling Setup page to determine how notification of the fatal, alert, warning, and information events should occur. You can choose to only count the events, display them to the console but not store them, record them after displaying them on the console, or notify someone of the occurrence after displaying and recording the event. Figure 7-10 shows the Event Handling Setup page.

Figure 7-10 The Event Handling Setup Page

Map Help Uptime: 02:50:48

Disposition of Events (by Severity Level)		Total Events
System Fatal	Notify	0
Protocol Fatal	Notify	0
Network Port Fatal	Notify	0
System Alert	Notify	0
Protocol Alert	Notify	0
Network Port Alert	Notify	0
External Alert	Notify	0
System Warning	Record	0
Protocol Warning	Record	581
Network Port Warning	Record	0
External Warning	Record	0
System Information	DisplayConsole	0
Protocol Information	Record	632
Network Port Information	Count	25
External Information	DisplayConsole	3

Handle **Station Alerts** as Severity Level External Information

Maximum memory reserved for **Detailed Event Trace Buffer** (bytes)

Download **Detailed Event Trace Buffer** [Headers Only](#) [All Data](#)

42913

Follow this link path to reach the Event Handling Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Event Handling** under Event Log.

Settings on the Event Handling Setup Page

The Event Handling Setup page contains the following settings:

- Disposition of Events
- Handle Station Events as Severity Level
- Maximum memory reserved for Detailed Event Trace Buffer (bytes)
- Download Detailed Event Trace Buffer
- Clear Alert Statistics
- Purge Trace Buffer

Disposition of Events

The event settings control how events are handled by the access point: counted, displayed in the log, recorded, or announced in a notification. The settings are color coded: red for fatal errors, magenta for alerts, blue for warnings, and green for information. You select an option from each setting's drop-down menu. Each option includes and builds upon the previous option.

- Count—Tallies the total events occurring in this category without any form of notification or display.
- Display Console—Provides a read-only display of the event but does not record it.
- Record—Makes a record of the event in the log and provides a read-only display of the event.
- Notify—Makes a record of the event in the log, displays the event, and tells the access point to notify someone of the occurrence.

Handle Station Events as Severity Level

You use this setting to set a severity level for Station Alerts. Use the drop-down menu to choose one of the sixteen severity levels. Table 7-2 on page 7-20 lists the severity levels in the menu. The *silent* option is not available for station events, however.

Maximum memory reserved for Detailed Event Trace Buffer (bytes)

Enter the number of bytes reserved for the Detailed Event Trace Buffer. The Detailed Event Trace Buffer is a tool for tracing the contents of packets between specified stations on your network.

After you reserve space for the trace buffer, browse to a device's Station page and select the **Alert** checkboxes in the To Station and From Station columns. See the "Browsing to Network Devices" section on page 9-2 for instructions on opening a device's Station page.

Download Detailed Event Trace Buffer

Use these links to view Headers Only or All Data in the detailed trace buffer. The number of bytes saved per packet is controlled on the Association Table Advanced Setup page.

If your browser is Netscape Communicator, click the links with your left mouse button to view the trace data. Click the links with your right mouse button and select **Save Link As** to save the data in a file.

Clear Alert Statistics

Click this button to reset the alert tallies to 0.

Purge Trace Buffer

Click this button to delete the packet traces from the Event Trace Buffer.

Event Notifications Setup Page

You use the Event Notifications Setup page to enable and configure notification of fatal, alert, warning, and information events to destinations external to the access point, such as an SNMP server or a Syslog system.



Note

For event notifications to be sent to an external destination, the events must be set to Notify on the Event Handling Setup page. See the “Event Handling Setup Page” section on page 7-21 for a description of the settings on the Event Handling Setup page.

Figure 7-11 shows the Event Notifications Setup page.

Figure 7-11 Event Notifications Setup Page

Map Help Uptime: 00:16:35

Should Notify-Disposition Events generate SNMP Traps? ☒ yes ☐ no

SNMP Trap Destination:

SNMP Trap Community:

Should Notify-Disposition Events generate Syslog Messages? ☒ yes ☐ no

Should Syslog Messages use the Cisco EMBLEM Format? ☒ yes ☐ no

Syslog Destination Address:

Network Default Syslog Destination: 0.0.0.0

Syslog Facility Number:

IEEE SNMP Traps should generate the following notifications:

Client Authentication Failure	Both IEEE Trap and Event Log
Client Deauthentication	Both IEEE Trap and Event Log
Client Disassociation	Both IEEE Trap and Event Log

Apply OK Cancel Restore Defaults 66313

Follow this link path to reach the Event Notifications Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Notifications** under Event Log.

Settings on the Event Notifications Setup Page

The Event Notifications Setup page contains the following settings:

- Should Notify-Disposition Events generate SNMP Traps?
- SNMP Trap Destination
- SNMP Trap Community
- Should Notify-Disposition Events generate Syslog Messages?
- Should Syslog Messages use the Cisco EMBLEM Format
- Syslog Destination Address
- Syslog Facility Number
- IEEE SNMP Traps Should Generate the Following Notifications

The page also displays the IP address of the network default syslog destination.

Should Notify-Disposition Events generate SNMP Traps?

Select **yes** to send event notifications to an SNMP server.



Note

For notifications to be sent to an SNMP server, SNMP must be enabled on the SNMP Setup page, and you must set an SNMP trap destination and an SNMP trap community.

SNMP Trap Destination

Type the IP address or the host name of the server running the SNMP Management software. This setting also appears on the SNMP Setup page.

SNMP Trap Community

Type the SNMP community name. This setting also appears on the SNMP Setup page.

Should Notify-Disposition Events generate Syslog Messages?

Select **yes** to send event notifications to a Syslog server.

Should Syslog Messages use the Cisco EMBLEM Format

When this setting is enabled, the access point generates EMBLEM (Baseline Manageability Specification) standard compliant system log messages:

```
ipaddress Counter: [yyy mmm dd hh:mm:ss TimeZone +/- hh:mm]: %FACILITY- SEVERITY-MNEMONIC:
Message-text
```

Example without timestamp:

```
192.168.12.83: %APBR-6-STA_ASSOC_OK: [AP350-12] Station [TEST-LPT]000750abcd2a Associated
```

Example with timestamp:

```
192.168.85:2002 SEP 12 13:52:12 PST -08:00: %APBR-6-STA_ASSOC_OK: [AP350-12] Station  
[TEST-LPT]000750abcd2a Associated
```

The timestamp is optional and included in the message only when the wall clock time is set on the access point. The facility code for all messages is APBR.

Syslog Destination Address

Type the IP address or the host name of the server running Syslog.

The Network Default Syslog Destination line under the syslog destination address field lists the syslog destination address provided by the DHCP or BOOTP server. This default syslog destination is only used if the syslog destination address field is blank.

Syslog Facility Number

Type the Syslog Facility number for the notifications. The default setting is 16, which corresponds to the Local0 facility code.

IEEE SNMP Traps Should Generate the Following Notifications

You can designate how the SNMP traps handles the following client events:

- Authentication failure
- Deauthentication
- Disassociation

You can set the following options for each event:

- No Trap nor Event Log—the event is neither trapped nor logged
- Event Log Only—the event is generated and sent to the event log only
- IEEE Trap Only—the event is trapped and sent to an SNMP community
- Both IEEE Trap and Event Log—the event is trapped and sent to the event log



Security Setup

This chapter describes how to set up your access point's security features. This chapter contains the following sections:

- Security Overview, page 8-2
- Setting Up WEP, page 8-9
- Enabling Additional WEP Security Features, page 8-13
- Setting Up Open or Shared Key Authentication, page 8-19
- Setting Up EAP Authentication, page 8-20
- Setting Up MAC-Based Authentication, page 8-29
- Summary of Settings for Authentication Types, page 8-37
- Setting Up Backup Authentication Servers, page 8-40
- Setting Up Administrator Authorization, page 8-41
- Setting up Centralized Administrator Authentication, page 8-45

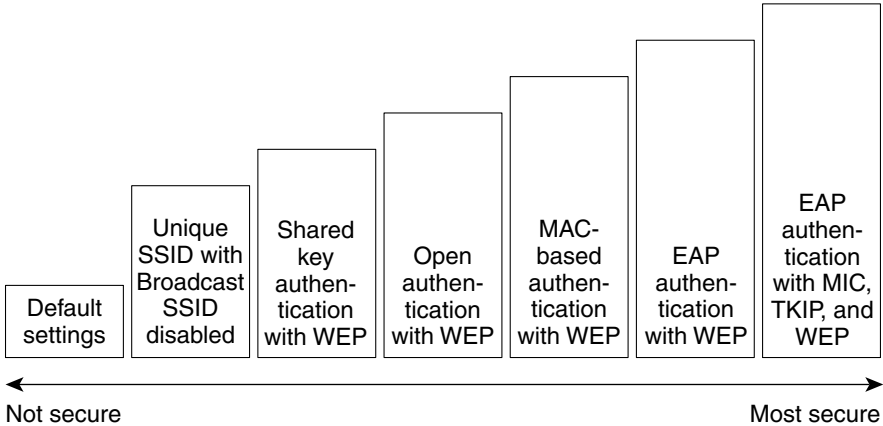
Security Overview

This section describes the types of security features you can enable on the access point. The security features protect wireless communication between the access point and other wireless devices, control access to your network, and prevent unauthorized entry to the access point management system.

Levels of Security

Security is vital for any wireless network, and you should enable all the security features available on your network. Figure 8-1 shows possible levels of security on Cisco Aironet wireless networking equipment, from no security on the left to highest security on the right. The highest level of security, EAP authentication, interacts with a Remote Authentication Dial-In User Service (RADIUS) server on your network to provide authentication service for wireless client devices.

Figure 8-1 *Wireless LAN Security Levels*



65677

If you don't enable any security features on your access point, anyone with a wireless networking device is able to join your network. If you enable open or shared-key authentication with WEP encryption, your network is safe from casual outsiders but vulnerable to intruders who use a hacking algorithm to calculate the WEP key. If you enable server-based EAP authentication with MIC, TKIP, and broadcast key rotation, your network is safe from all but the most sophisticated attacks against wireless security.

Encrypting Radio Signals with WEP

Just as anyone within range of a radio station can tune to the station's frequency and listen to the signal, any wireless networking device within range of an access point can receive the access point's radio transmissions. Because WEP (Wired Equivalent Privacy) is the first line of defense against intruders, Cisco recommends that you use full encryption on your wireless network.

WEP encryption scrambles the communication between the access point and client devices to keep the communication private. Both the access point and client devices use the same WEP key to encrypt and unencrypt radio signals. WEP keys encrypt both unicast and multicast messages. Unicast messages are addressed to just one device on the network. Multicast messages are addressed to multiple devices on the network.

Extensible Authentication Protocol (EAP) authentication provides dynamic WEP keys to wireless users. Dynamic WEP keys are more secure than static, or unchanging, WEP keys. If an intruder passively receives enough packets encrypted by the same WEP key, the intruder can perform a calculation to learn the key and use it to join your network. Because they change frequently, dynamic WEP keys prevent intruders from performing the calculation and learning the key.

Additional WEP Security Features

Three additional security features defend your wireless network's WEP keys:

- Message Integrity Check (MIC)—MIC prevents attacks on encrypted packets called *bit-flip* attacks. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC, implemented on both the access point and all associated client devices, adds a few bytes to

each packet to make the packets tamper-proof. See the “Enabling Message Integrity Check (MIC)” section on page 8-14 for instructions on enabling MIC. MIC is also known as key hashing.

- **TKIP (Temporal Key Integrity Protocol, also known as WEP key hashing)**—This feature defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. See the “Enabling Temporal Key Integrity Protocol (TKIP)” section on page 8-16 for instructions on enabling TKIP.
- **Broadcast key rotation**—EAP authentication provides dynamic unicast WEP keys for client devices but uses static broadcast, or multicast, keys. When you enable broadcast WEP key rotation, the access point provides a dynamic broadcast WEP key and changes it at the interval you select. Broadcast key rotation is an excellent alternative to TKIP if your wireless LAN supports wireless client devices that are not Cisco devices or that cannot be upgraded to the latest firmware for Cisco client devices. See the “Enabling Broadcast WEP Key Rotation” section on page 8-18 for instructions on enabling broadcast key rotation.

**Note**

The MIC, TKIP, and broadcast key rotation features are available in firmware versions 11.10T and later, which are available on Cisco.com. You can download Cisco Aironet firmware releases at <http://www.cisco.com/public/sw-center/sw-wireless.shtml>.

Network Authentication Types

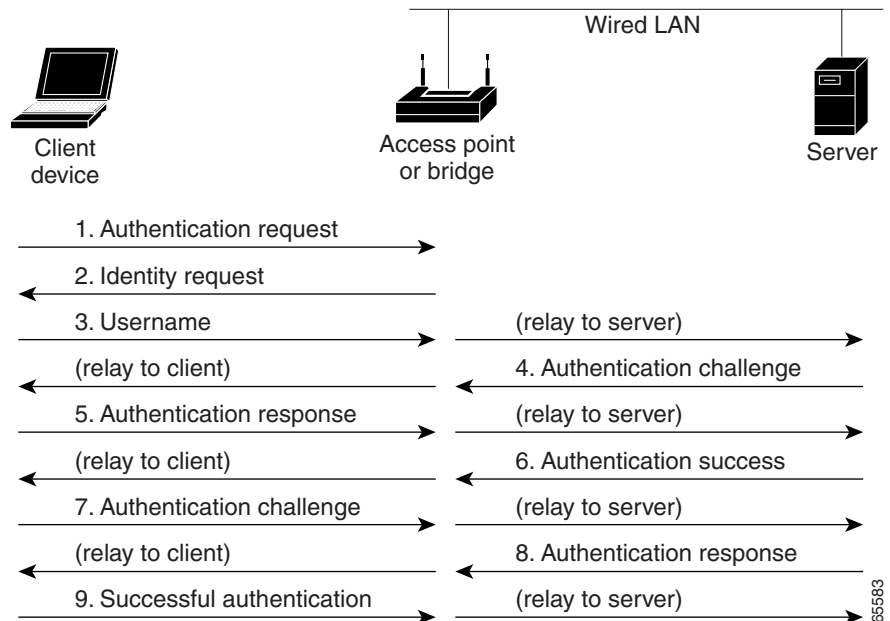
Before a wireless client device can communicate on your network through the access point, it must authenticate to the access point and to your network. The access point uses four authentication mechanisms or types and can use more than one at the same time:

- **Network-EAP**—This authentication type provides the highest level of security for your wireless network. By using the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. The RADIUS

server sends the WEP key to the access point, which uses it for all unicast data signals that it sends to or receives from the client. The access point also encrypts its broadcast WEP key (entered in the access point's WEP key slot 1) with the client's unicast key and sends it to the client.

When you enable EAP on your access points and client devices, authentication to the network occurs in the steps shown in Figure 8-2:

Figure 8-2 Sequence for EAP Authentication



In steps 1 through 9 in Figure 8-2, a wireless client device and a RADIUS server on the wired LAN use 802.1X and EAP to perform a mutual authentication through the access point. The RADIUS server sends an authentication challenge to the client. The client uses a one-way encryption of the user-supplied password to generate a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, and the client authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the client determine a WEP key that is unique to the client and provides the client with the appropriate level of network access, thereby approximating the level of security in a wired switched segment to an individual desktop. The client loads this key and prepares to use it for the logon session.

During the logon session, the RADIUS server encrypts and sends the WEP key, called a *session key*, over the wired LAN to the access point. The access point encrypts its broadcast key with the session key and sends the encrypted broadcast key to the client, which uses the session key to decrypt it. The client and access point activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.

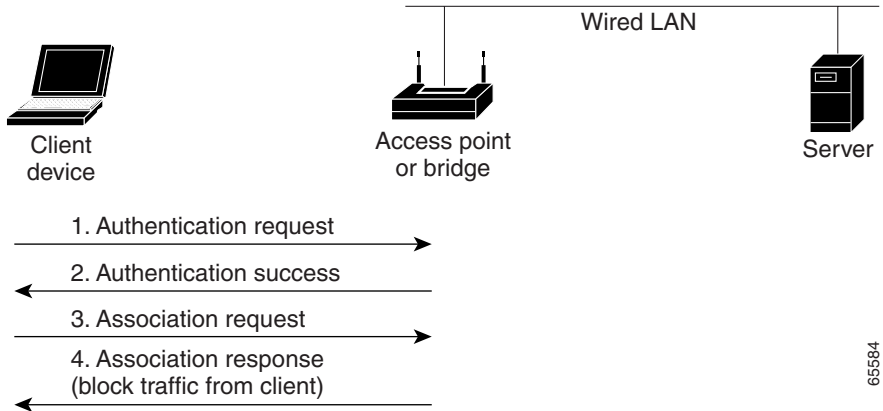
There is more than one type of EAP authentication, but the access point behaves the same way for each type: it relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device. See the “Setting Up EAP Authentication” section on page 8-20 for instructions on setting up EAP on the access point.

**Note**

If you use EAP authentication, you can select open or shared key authentication, but you don't have to. EAP authentication controls authentication both to your access point and to your network.

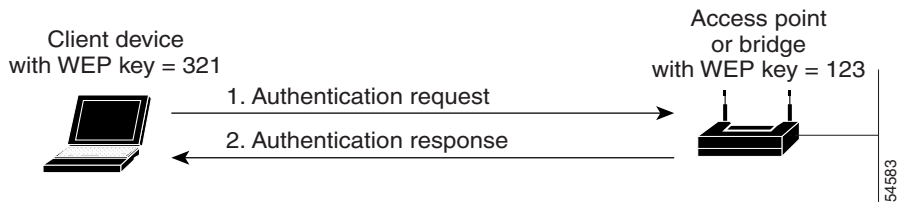
- **MAC address**—The access point relays the wireless client device's MAC address to a RADIUS server on your network, and the server checks the address against a list of allowed MAC addresses. If you don't have a RADIUS server on your network, you can create the list of allowed MAC addresses on the access point's Address Filters page. Devices with MAC addresses not on the list are not allowed to authenticate. Intruders can create counterfeit MAC addresses, so MAC-based authentication is less secure than EAP authentication. However, MAC-based authentication provides an alternate authentication method for client devices that do not have EAP capability. See the “Setting Up MAC-Based Authentication” section on page 8-29 for instructions on enabling MAC-based authentication.

Figure 8-3 shows the authentication sequence for MAC-based authentication.

Figure 8-3 Sequence for MAC-Based Authentication

- Open—Allows any device to authenticate and then attempt to communicate with the access point. Using open authentication, any wireless device can authenticate with the access point, but the device can only communicate if its WEP keys match the access point's. Devices not using WEP do not attempt to authenticate with an access point that is using WEP. Open authentication does not rely on a RADIUS server on your network.

Figure 8-4 shows the authentication sequence between a device trying to authenticate and an access point using open authentication. In this example, the device's WEP key does not match the access point's key, so it can authenticate but not pass data.

Figure 8-4 Sequence for Open Authentication

- Shared key—Cisco provides shared key authentication to comply with the IEEE 802.11b standard. However, because of shared key's security flaws, we recommend that you avoid using it.

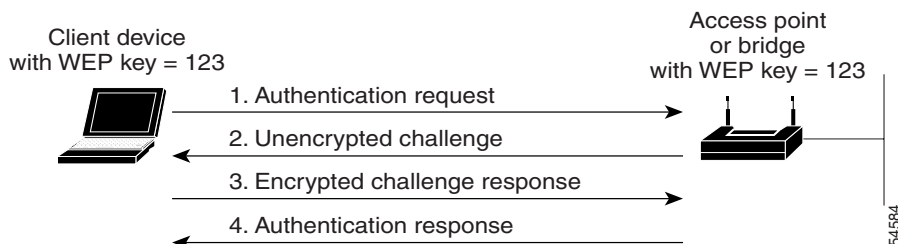
During shared key authentication, the access point sends an unencrypted challenge text string to any device attempting to communicate with the access point. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. Both the unencrypted challenge and the encrypted challenge can be monitored, however, which leaves the access point open to attack from an intruder who calculates the WEP key by comparing the unencrypted and encrypted text strings. Because of this weakness, shared key authentication can be less secure than open authentication. Like open authentication, shared key authentication does not rely on a RADIUS server on your network.

Figure 8-5 shows the authentication sequence between a device trying to authenticate and an access point using shared key authentication. In this example the device's WEP key matches the access point's key, so it can authenticate and communicate.

**Note**

You cannot enable MIC and TKIP for SSIDs that use shared key authentication.

Figure 8-5 Sequence for Shared Key Authentication



Combining MAC-Based, EAP, and Open Authentication

You can set up the access point to authenticate client devices using a combination of MAC-based and EAP authentication. When you enable this feature, client devices that associate to the access point using 802.11 open authentication first attempt MAC authentication; if MAC authentication succeeds, the client device joins the network. If MAC authentication fails, the access point waits for the client

device to attempt EAP authentication. See the “Authenticating Client Devices Using MAC Addresses or EAP” section on page 8-34 for more information on this feature.

Protecting the Access Point Configuration with User Manager

The access point’s user manager feature prevents unauthorized entry to the access point management system. You create a list of administrators authorized to view and adjust the access point settings; unauthorized users are locked out. See the “Setting Up Administrator Authorization” section on page 8-41 for instructions on using the user manager.

Setting Up WEP

Use the AP Radio Data Encryption page to set up WEP. You also use the AP Radio Data Encryption page to select an authentication type for the access point. Figure 8-6 shows the AP Radio Data Encryption page.

Figure 8-6 AP Radio Data Encryption Page

Map Help Uptime: 1 day, 06:32:43

If VLANs are *not* enabled, set Radio Data Encryption on this page. If VLANs *are* enabled, Radio Data Encryption is set independently for each enabled VLAN through [VLAN Setup](#).

Use of Data Encryption by Stations is: Not Available
Must set an Encryption Key or enable Broadcast Key Rotation first

	Open	Shared	Network-EAP
Accept Authentication Type:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Require EAP:	<input type="checkbox"/>	<input type="checkbox"/>	

	Transmit With Key	Encryption Key	Key Size
WEP Key 1:	-	<input type="text"/>	not set ▼
WEP Key 2:	-	<input type="text"/>	not set ▼
WEP Key 3:	-	<input type="text"/>	not set ▼
WEP Key 4:	-	<input type="text"/>	not set ▼

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
 Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
 This radio supports Encryption for all Data Rates.

Apply OK Cancel Restore Defaults

49506

Follow this link path to reach the AP Radio Data Encryption page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Security**.
3. On the Security Setup page, click **Radio Data Encryption (WEP)**.

**Note**

Use this page to configure the radio unless you have enabled VLANs. If VLANs are enabled, you must set the radio data encryption for each enabled VLAN through the VLAN Setup page.

Follow these steps to set up WEP keys and enable WEP:

Step 1 Follow the link path to the AP Radio Data Encryption page.

Step 2 Before you can enable WEP, you must enter a WEP key in at least one of the Encryption Key fields.

**Note**

If you enable broadcast key rotation and EAP authentication to provide client devices with dynamic WEP keys, you can enable WEP without entering the keys.

For 40-bit encryption, enter 10 hexadecimal digits; for 128-bit encryption, enter 26 hexadecimal digits. Hexadecimal digits include the numbers 0 through 9 and the letters A through F. Your 40-bit WEP keys can contain any combination of 10 of these characters; your 128-bit WEP keys can contain any combination of 26 of these characters. The letters are not case-sensitive.

You can enter up to four WEP keys. The characters you type for a key's contents appear only when you type them. After you click **Apply** or **OK**, you cannot view the key's contents.

**Note**

If you enable EAP authentication, you must select key 1 as the transmit key. The access point uses the WEP key you enter in key slot 1 to encrypt multicast data signals it sends to EAP-enabled client devices. If you enable broadcast key rotation, however, you can select key 1 or key 2 as the transmit key or you can enable WEP without entering any keys.

- Step 3** Use the Key Size pull-down menu to select **40-bit** or **128-bit** encryption for each key. The **not set** option clears the key. You can disable WEP altogether by selecting **not set** for each key or by selecting **No Encryption** in Step 5.
- Step 4** Select one of the keys as the transmit key. If you select Network-EAP as the authentication type, select key 1 as the transmit key.

**Note**

Client devices that do not use EAP to authenticate to the access point must contain the access point's transmit key in the same key slot in the client devices' WEP key lists. If MIC is also enabled on the access point, the key must also be selected as the transmit key in the client devices' WEP key lists.

Table 8-1 shows an example WEP key setup that would work for the access point and an associated device:

Table 8-1 WEP Key Setup Example

Key Slot	Access Point		Associated Device	
	Transmit?	Key Contents	Transmit?	Key Contents
1	x	12345678901234567890abcdef	—	12345678901234567890abcdef
2	—	09876543210987654321fedcba	x	09876543210987654321fedcba
3	—	not set	—	not set
4	—	not set	—	FEDCBA09876543211234567890

Because the access point's WEP key 1 is selected as the transmit key, WEP key 1 on the other device must contain the same contents. WEP key 4 on the other device is set, but because it is not selected as the transmit key, WEP key 4 on the access point does not need to be set at all.

The characters you type for the key contents appear only when you type them. After you click **Apply** or **OK**, you cannot view the key contents. Select **Not set** from the Key Size pull-down menu to clear a key.

- Step 5** Select **Optional** or **Full Encryption** from the pull-down menu labeled *Use of Data Encryption by Stations is*.



Note You must set a WEP key before enabling WEP. The options in the *Use of Data Encryption by Stations* pull-down menu do not appear until you set a key.

The three settings in the pull-down menu include:

- No Encryption (default)—The access point communicates only with client devices that are not using WEP. Use this option to disable WEP.
- Optional—Client devices can communicate with the access point either with or without WEP.



Note If you select Optional, Cisco Aironet client devices associating to the access point must be configured to allow association to mixed cells. See the *Cisco Aironet Wireless LAN Adapters Software Configuration Guide* for instructions on configuring Cisco Aironet client devices.

- Full Encryption—Client devices must use WEP when communicating with the access point. Devices not using WEP are not allowed to communicate.



Note You must select Full Encryption to enable Message Integrity Check (MIC). See the “Enabling Message Integrity Check (MIC)” section on page 8-14 for instructions on setting up MIC.

Step 6 Click **OK**. You return automatically to the Security Setup page.

Using SNMP to Set Up WEP

You can use SNMP to set the WEP level on the access point. Consult the “Using SNMP” section on page 2-24 for details on using SNMP.

Access points use the following SNMP variables to set the WEP level:

- dot11ExcludeUnencrypted.2
- awcDot11AllowEncrypted.2

Table 8-2 lists the SNMP variable settings and the corresponding WEP levels.

Table 8-2 *SNMP Variable Settings and Corresponding WEP Levels*

SNMP Variable	WEP Full	WEP Off	WEP Optional
dot11ExcludeUnencrypted.2	true	false	false
awcDot11AllowEncrypted.2	true	false	true

**Note**

Access points do not use the SNMP variable *dot11PrivacyInvoked*, so it is always set to disabled.

Enabling Additional WEP Security Features

You can enable three advanced security features to protect against sophisticated attacks on your wireless network’s WEP keys. This section describes how to set up and enable these features:

- Enabling Message Integrity Check (MIC)
- Enabling Temporal Key Integrity Protocol (TKIP)
- Enabling Broadcast WEP Key Rotation

**Note**

The MIC, TKIP, and broadcast key rotation features are available in firmware versions 11.10T and later, which are available on Cisco.com. You can download Cisco Aironet firmware releases at <http://www.cisco.com/public/sw-center/sw-wireless.shtml>.

Enabling Message Integrity Check (MIC)

MIC prevents attacks on encrypted packets called *bit-flip* attacks. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC, implemented on both the access point and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof.

**Note**

You must set up and enable WEP with full encryption before MIC takes effect.

**Note**

To use MIC, the Use Aironet Extensions setting on the AP Radio Advanced page must be set to yes (the default setting).

Use the AP Radio Advanced page to enable MIC. Figure 8-7 shows the AP Radio Advanced page.

Figure 8-7 AP Radio Advanced Page

Uptime: 3 days, 17:01:17

Map Help

Requested Status:	<input type="button" value="Up"/>
Current Status:	Up
Packet Forwarding:	<input type="button" value="Enabled"/>
Forwarding State:	Forwarding
Default Multicast Address Filter:	<input type="button" value="Allowed"/>
Maximum Multicast Packets/Second:	<input type="text" value="0"/>

Radio Cell Role:	<input type="button" value="Access Point/Root"/>
SSID for use by Infrastructure Stations (such as Repeaters):	<input type="text" value="0"/>
Disallow Infrastructure Stations on any <i>other</i> SSID:	<input type="radio"/> yes <input checked="" type="radio"/> no
Use Aironet Extensions:	<input checked="" type="radio"/> yes <input type="radio"/> no
Classify Workgroup Bridges as Network Infrastructure:	<input checked="" type="radio"/> yes <input type="radio"/> no
Require use of Radio Firmware 4.99H:	<input checked="" type="radio"/> yes <input type="radio"/> no
Ethernet Encapsulation Transform:	<input type="button" value="RFC1042"/>

Quality of Service Setup

If VLANs are *not* enabled, set the following three parameters on this page. If VLANs *are* enabled, the following three parameters are set independently for each enabled VLAN through VLAN Setup.

Enhanced MIC verification for WEP:	<input type="button" value="None"/>
Temporal Key Integrity Protocol:	<input type="button" value="None"/>
Broadcast WEP Key rotation interval (sec):	<input type="text" value="0"/> (0=off)

To configure 802.11 Authentication, EAP, Unicast Address Filters, and the Maximum Number of Associations for this radio's Primary SSID (the default SSID), please use the link below.

Advanced Primary SSID Setup

Specified Access Point 1:	<input type="text" value="00:00:00:00:00:00"/>
Specified Access Point 2:	<input type="text" value="00:00:00:00:00:00"/>
Specified Access Point 3:	<input type="text" value="00:00:00:00:00:00"/>
Specified Access Point 4:	<input type="text" value="00:00:00:00:00:00"/>

Radio Modulation:	<input type="button" value="Standard"/>
Radio Preamble:	<input type="button" value="Short"/>

81735

Follow this link path to browse to the AP Radio Advanced page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Advanced** in the AP Radio row under Network Ports.

Follow these steps to enable MIC:

- Step 1** Follow the steps in the “Setting Up WEP” section on page 8-9 to set up and enable WEP. You must set up and enable WEP with full encryption before MIC becomes active. If WEP is off or if you set it to optional, MIC is not enabled.



Note If you enable MIC but you use static WEP (you do not enable any type of EAP authentication), both the access point and any devices with which it communicates must use the same WEP key for transmitting data. For example, if the MIC-enabled access point uses the key in slot 1 as the transmit key, a client device associated to the access point must use the same key in its slot 1, and the key in the client’s slot 1 must be selected as the transmit key.



Note You cannot enable MIC and TKIP for SSIDs that used shared key authentication.

- Step 2** Browse to the AP Radio Advanced page.
- Step 3** Select **MMH** from the Enhanced MIC verification for WEP pull-down menu.
- Step 4** Make sure **yes** is selected for the Use Aironet Extensions setting. MIC does not work if Use Aironet Extensions is set to no.
- Step 5** Click **OK**. MIC is enabled, and only client devices with MIC capability can communicate with the access point.

Enabling Temporal Key Integrity Protocol (TKIP)

Temporal Key Integrity Protocol (TKIP), also known as WEP key hashing, defends against an attack on WEP in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. TKIP protects both unicast and broadcast WEP keys.

**Note**

When you enable TKIP, all WEP-enabled client devices associated to the access point must support WEP key hashing. WEP-enabled devices that do not support key hashing cannot communicate with the access point.

**Note**

To use TKIP, the Use Aironet Extensions setting on the AP Radio Advanced page must be set to **yes** (the default setting).

**Tip**

When you enable TKIP, you might not need to enable broadcast key rotation. Key hashing prevents intruders from calculating the static broadcast key, so you do not need to rotate the broadcast key.

**Note**

You cannot enable MIC and TKIP for SSIDs that use shared key authentication.

Follow these steps to enable TKIP:

-
- Step 1** Follow the steps in the “Setting Up WEP” section on page 8-9 to set up and enable WEP. Select either optional or full encryption for the WEP level.
- Step 2** Follow this link path to browse to the AP Radio Advanced page:
- a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **Advanced** in the AP Radio row under Network Ports.
- Step 3** Select **Cisco** from the Temporal Key Integrity Protocol pull-down menu.
- Step 4** Make sure **yes** is selected for the Use Aironet Extensions setting. Key hashing does not work if Use Aironet Extensions is set to no.
- Step 5** Click **OK**. TKIP is enabled.
-

Enabling Broadcast WEP Key Rotation

EAP authentication provides dynamic unicast WEP keys for client devices but uses static multicast keys. With broadcast, or multicast, WEP key rotation enabled, the access point provides a dynamic broadcast WEP key and changes it at the interval you select. Broadcast key rotation is an excellent alternative to TKIP if your wireless LAN supports wireless client devices that are not Cisco devices or that cannot be upgraded to the latest firmware for Cisco client devices.

**Note**

When you enable broadcast key rotation, only wireless client devices using LEAP or EAP-TLS authentication can use the access point. Client devices using static WEP (with open, shared key, or EAP-MD5 authentication) cannot use the access point when you enable broadcast key rotation.

**Tip**

Broadcast key rotation and TKIP (WEP key hashing) provide similar protection. If you enable TKIP, you might not need to enable key rotation.

Follow these steps to enable broadcast key rotation:

- Step 1** Follow the steps in the “Setting Up WEP” section on page 8-9 to set up and enable WEP.
- Step 2** Follow this link path to browse to the AP Radio Advanced page:
 - a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **Advanced** in the AP Radio row under Network Ports.
- Step 3** On the AP Radio Advanced page, enter the rotation interval in seconds in the Broadcast WEP Key rotation interval entry field. If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. To disable broadcast WEP key rotation, enter **0**.

**Note**

You must set the rotation interval on every access point using broadcast key rotation. You cannot enter the rotation interval on your RADIUS server.

**Tip**

Use a short rotation interval if the traffic on your wireless network contains numerous broadcast or multicast packets.

Step 4 Click **OK**. Broadcast key rotation is enabled.

Setting Up Open or Shared Key Authentication

Cisco recommends Open authentication as preferable to Shared Key authentication. The challenge queries and responses used in Shared Key leave the access point particularly vulnerable to intruders.

Use the AP Radio Data Encryption page to select Open or Shared Key authentication. Figure 8-6 shows the AP Radio Data Encryption page.

Follow these steps to select Open or Shared Key authentication:

Step 1 Follow the instructions in the “Setting Up WEP” section on page 8-9 to set up and enable WEP.

You must enable WEP to use shared key authentication, but you do not have to enable WEP to use open authentication. However, Cisco strongly recommends that you enable WEP on all wireless networks.

Step 2 Select **Open** (default) or **Shared Key** to set the authentications the access point recognizes. You can select all three authentication types.

Step 3 If you want to force all client devices to perform EAP authentication before joining the network, select the **Require EAP** checkbox under Open or Shared. Selecting the Require EAP checkbox also allows client devices using various types of EAP authentication, including EAP-TLS and EAP-MD5, to authenticate through the access point. To allow LEAP-enabled client devices to authenticate through the access point, you should also select **Network-EAP**. See the “Setting Up EAP Authentication” section on page 8-20 for details on the Require EAP and Network-EAP settings.

Step 4 Click **OK**. You return automatically to the Security Setup page.

Setting Up EAP Authentication

During EAP authentication, the access point relays authentication messages between the RADIUS server on your network and the authenticating client device. This section provides instructions for:

- Enabling EAP on the Access Point
- Enabling EAP in Cisco Secure ACS
- Setting up a Repeater Access Point as a LEAP Client

Enabling EAP on the Access Point

You use the Authenticator Configuration page and the AP Radio Data Encryption page to set up and enable EAP authentication. Figure 8-6 shows the AP Radio Data Encryption page. Figure 8-8 shows the Authenticator Configuration page.

Figure 8-8 Authenticator Configuration Page

Map

Help

Uptime: 1 day, 19:55:08

802.1X Protocol Version (for EAP Authentication):

802.1x-2001

Primary Server Reattempt Period (Min.):

0

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran
	RADIUS	1812		5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
	RADIUS	1812		5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
	RADIUS	1812		5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
	RADIUS	1812		5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					

Note: For each authentication function, the most recently used server is shown in green text.

Apply

OK

Cancel

Restore Defaults

66565

Follow this link path to reach the Authenticator Configuration page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Security**.
3. On the Security Setup page, click **Authentication Server**.

Follow these steps to enable EAP on the access point:

Step 1 Follow the link path to the Authenticator Configuration page.

You can configure up to four servers for authentication services, so you can set up backup authenticators. If you set up more than one server for the same service, the server first in the list is the primary server for that service, and the others are used in list order when the previous server times out.



Note You can use the same server for both EAP authentication and MAC-address authentication.

Step 2 Use the 802.1X Protocol Version (for EAP authentication) pull-down menu to select the draft of the 802.1X protocol the access point's radio will use. EAP operates only when the radio firmware on client devices complies with the same 802.1X Protocol draft as the management firmware on the access point. If the radio firmware on the client devices that will associate with the access point is 4.16, for example, you should select **Draft 8**. Menu options include:

- Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting.
- Draft 8—Select this option if LEAP-enabled client devices that associate with this access point use radio firmware versions 4.13, 4.16, or 4.23.
- 802.1x-2001 (formerly Draft 10)—Select this option if client devices that associate with this access point use Microsoft Windows XP authentication or if LEAP-enabled client devices that associate with this access point use radio firmware version 4.25 or later.

Table 8-3 lists the radio firmware versions and the drafts with which they comply.

Table 8-3 802.1X Protocol Drafts and Compliant Client Firmware

Firmware Version	Draft 7	Draft 8	802.1x-2001
PC/PCI cards 4.13	—	x	—
PC/PCI cards 4.16	—	x	—
PC/PCI cards 4.23	—	x	—
PC/PCI cards 4.25 and later	—	—	x
WGB34x/352 8.58	—	x	—
WGB34x/352 8.61 or later	—	—	x
AP34x/35x 11.05 and earlier	—	x	—
AP34x/35x 11.06 and later ¹	—	x	x
BR352 11.06 and later ¹	—	x	x

1. The default draft setting in access point and bridge firmware version 11.06 and later is 802.1x-2001.

**Note**

Draft standard 8 is the default setting in firmware version 11.05 and earlier, and it might remain in effect when you upgrade the firmware to version 11.06 or later. Check the setting on the Authenticator Configuration page in the management system to make sure the best draft standard for your network is selected.

- Step 3** Enter the name or IP address of the RADIUS server in the Server Name/IP entry field.
- Step 4** Enter the port number your RADIUS server uses for authentication. The default setting, *1812*, is the port setting for Cisco's RADIUS server, the Cisco Secure Access Control Server (ACS), and for many other RADIUS servers. Check your server's product documentation to find the correct port setting.
- Step 5** Enter the shared secret used by your RADIUS server in the Shared Secret entry field. The shared secret on the access point must match the shared secret on the RADIUS server. The shared secret can contain up to 64 alphanumeric characters.
- Step 6** Enter the number of seconds the the access point should wait before authentication fails.

- Step 7** Enter the number of seconds the access point should wait before authentication fails. If the server does not respond within this time, the access point tries to contact the next authentication server in the list if one is specified. Other backup servers are used in list order when the previous server times out.
- Step 8** Select **EAP Authentication** under the server. The EAP Authentication checkbox designates the server as an authenticator for any EAP type, including LEAP, EAP-TLS, and EAP-MD5.
- Step 9** Click **OK**. You return automatically to the Security Setup page.
- Step 10** On the Security Setup page, click **Radio Data Encryption (WEP)** to browse to the AP Radio Data Encryption page.
- Step 11** Select **Network-EAP** for the Authentication Type setting to allow EAP-enabled client devices to authenticate through the access point.

Select **Require EAP** under Open or Shared Key to allow client devices with EAP-TLS or EAP-MD5 enabled through Windows XP to authenticate through the access point. If you do not select Require EAP, client devices with EAP enabled through Windows XP authenticate to the access point but might not perform mutual EAP authentication with your RADIUS server. LEAP-enabled client devices perform LEAP authentication through the access point even if you do not select Require EAP.



Note When you select Require EAP, you block client devices that are not using EAP from authenticating through the access point.

Table 8-4 lists the access point settings that provide authentication for various client devices.

Table 8-4 Access Point EAP Settings for Various Client Configurations

Access Point Configuration	Client Devices Allowed to Authenticate
Network-EAP authentication	<ul style="list-style-type: none"> Client devices with LEAP enabled Repeater access points with LEAP enabled
Open authentication with Require EAP checkbox selected	<ul style="list-style-type: none"> Client devices with EAP enabled Cisco Aironet devices with EAP-TLS or EAP-MD5 enabled through Windows XP <p>Note Selecting Require EAP on the access point blocks non-EAP client devices from using the access point.</p>

Step 12 Check that a WEP key has been entered in key slot 1. If a WEP key has been set up in slot 1, skip to Step 16. If no WEP key has been set up, proceed to Step 13.



Note You can use EAP without enabling WEP, but packets sent between the access point and the client device will not be encrypted. To maintain secure communications, use WEP at all times.

Step 13 Enter a WEP key in slot 1 of the Encryption Key fields. The access point uses this key for multicast data signals (signals sent from the access point to several client devices at once). This key does not need to be set on client devices.

Step 14 Select **128-bit** encryption from the Key Size pull-down menu.

Step 15 If the key in slot 1 is the only WEP key set up, select it as the transmit key.

Step 16 Click **OK**. You return automatically to the Security Setup page.

Enabling EAP in Cisco Secure ACS

Cisco Secure Access Control Server for Windows NT/2000 Servers (Cisco Secure ACS) is network security software that helps authenticate users by controlling access to a network access server (NAS) device, such as an access server, PIX Firewall, router, or wireless access point or bridge.

Cisco Secure ACS operates as a Windows NT or Windows 2000 service and controls the authentication, authorization, and accounting (AAA) of users accessing networks. Cisco Secure ACS operates with Windows NT 4.0 Server and Windows 2000 Server.

**Note**

You must use ACS version 2.6 or later to set up the access point in ACS.

Follow these steps to include the access point as a Network Access Server (NAS) in Cisco Secure ACS:

-
- Step 1** On the ACS main menu, click **Network Configuration**.
 - Step 2** Click **Add New Access Server**.
 - Step 3** In the **Network Access Server Hostname** entry field, type the name you want to assign to the access point as an access server.

**Note**

This field does not appear if you are configuring an existing NAS.

- Step 4** In the **Network Access Server IP address** box, type the access point's IP address.
- Step 5** In the **Key** box, type the shared secret that the TACACS+ or RADIUS NAS and Cisco Secure ACS use to encrypt the data. For correct operation, the identical key (case sensitive) must be configured on the access point's Authenticator Configuration page and in Cisco Secure ACS.
- Step 6** From the **Authenticate Using** drop-down menu, select **RADIUS (Cisco Aironet)**.
- Step 7** To save your changes and apply them immediately, click the **Submit + Restart** button.

**Tip**

To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, select **System Configuration > Service Control** and click **Restart**.

**Note**

Restarting the service clears the Logged-in User Report, refreshes the Max Sessions counter, and temporarily interrupts all Cisco Secure ACS services.

Setting a Session-Based WEP Key Timeout

You can set a timeout value for the session-based WEP key. When the timeout value elapses, the server issues a new dynamic WEP key for authenticated client devices.

**Note**

If you enable TKIP (WEP key hashing) on the access point, you do not need to set up a session-based WEP key timeout. You can use both TKIP and a session key timeout, but these features provide redundant protection.

You should consider several factors when determining the best session key timeout value for your wireless network. Consult *Product Bulletin 1515: Cisco Wireless LAN Security Bulletin* for guidelines on selecting timeout values. Use this URL to browse to Product Bulletin 1515:

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515_pp.htm

Follow these steps to set a timeout value for session-based WEP keys:

- Step 1** On the ACS main menu, click **Group Setup**.
- Step 2** In the Group drop-down menu, select the group for which you want to modify the WEP key/session timeout. The **Default** group is usually the group you need to modify.
- Step 3** Click **Edit Settings**.

- Step 4** Scroll down to the IETF RADIUS Attributes settings.
 - Step 5** Select the checkbox for [027] Session-Timeout and enter the number of seconds for your timeout value in the [027] Session-Timeout entry field.
 - Step 6** Click **Submit + Restart**. The timeout value is enabled.
-

Setting up a Repeater Access Point as a LEAP Client

If you configure your access point as a repeater (an access point not connected to the wired LAN), you can set up the repeater access point to authenticate to your network like other wireless client devices. After you provide a network username and password for the repeater access point, it authenticates to your network using LEAP, Cisco's wireless authentication method, and receives and uses dynamic WEP keys.

See the “Setting Up a Repeater Access Point” section on page 12-2 for instructions on setting up a repeater access point.

Follow these steps to enable LEAP authentication on a repeater access point:

-
- Step 1** Set up a username and password on your network just as you would for a new user. The repeater access point will use this username and password to authenticate.
 - Step 2** Follow this link path to browse to the AP Radio Identification page:
 - a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **Identification** in the AP Radio row under Network Ports.

Figure 8-9 shows the AP Radio Identification page.

Figure 8-9 AP Radio Identification Page

- Step 3** Enter the network username you set up for the access point in Step 1 in the LEAP User Name entry field.
- Step 4** Enter the network password you set up for the access point in Step 1 in the LEAP Password entry field.
- Step 5** Click **OK**.
- Step 6** Follow the steps in the “Enabling EAP on the Access Point” section on page 8-20 to enable Network-EAP on the repeater access point.

The next time the repeater reboots, it performs LEAP authentication and associates to the root access point.



Note If the repeater access point fails to authenticate because the root access point or the RADIUS server is not set up correctly, you must reboot the repeater access point after correcting the problem. The repeater access point does not attempt to reauthenticate until it reboots.

Setting Up MAC-Based Authentication

MAC-based authentication allows only client devices with specified MAC addresses to associate and pass data through the access point. Client devices with MAC addresses not in a list of allowed MAC addresses are not allowed to associate with the access point. You can create a list of allowed MAC addresses in the access point management system and on a server used for MAC-based authentication.

This section provides instructions for:

- Enabling MAC-Based Authentication on the Access Point
- Authenticating Client Devices Using MAC Addresses or EAP
- Enabling MAC-Based Authentication in Cisco Secure ACS

Enabling MAC-Based Authentication on the Access Point

Follow these steps to set up and enable MAC-based authentication on the access point:

-
- Step 1** Follow this link path to reach the Address Filters page:
- a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **Address Filters** under Associations.

Figure 8-10 shows the Address Filters page.

Figure 8-10 Address Filters Page

Map Help Uptime: 6 days, 22:56:46

New MAC Address Filter:

Dest MAC Address:

☒ Allowed ☐ Disallowed

The default settings for multicast and unicast destination MAC addresses transmitted from each network interface are specified on the Advanced Setup page for that network interface.

Existing MAC Address Filters:

Lookup MAC Address on [Authentication Server](#) if not in Existing Filter List? ☐ yes ☒ no

Is MAC Authentication alone sufficient for a client to be fully authenticated? ☐ yes ☒ no

49993

**Note**

Step 2 and Step 3 describe entering MAC addresses in the access point management system. If you will enter MAC addresses only in a list used by the authentication server, skip to Step 4.

- Step 2** Type a MAC address in the Dest MAC Address field. You can type the address with colons separating the character pairs (00:40:96:12:34:56, for example) or without any intervening characters (004096123456, for example).

Make sure the **Allowed** option is selected under the Dest MAC Address field.

- Step 3** Click **Add**. The MAC address appears in the Existing MAC Address Filters list. The MAC address remains in the management system until you remove it. To remove the MAC address from the list, select it and click **Remove**.

**Note**

Be sure to enter your own MAC address in the list of allowed addresses.

- Step 4** If you plan to create a MAC address list that will be checked by the authentication server, select **Yes** for the option called Lookup MAC Address on Authentication Server if not in Existing Filter List. With this option enabled, the access point checks the authentication server's MAC address list when a client device attempts to authenticate.
- Step 5** Click **Apply** to save the list of MAC addresses in the access point management system.
- Step 6** Click the **Authentication Server** link to go to the Authenticator Configuration page. Figure 8-11 shows the Authenticator Configuration page.

Figure 8-11 Authenticator Configuration Page

The screenshot shows the 'Authenticator Configuration' page. At the top left are 'Map' and 'Help' buttons. At the top right is the 'Uptime: 1 day, 19:55:08' status. Below these are two settings: '802.1X Protocol Version (for EAP Authentication):' set to '802.1x-2001' and 'Primary Server Reattempt Period (Min.):' set to '0'. The main section contains a table with four rows, each representing an authentication server. The columns are: 'Server Name/IP', 'Server Type' (all set to 'RADIUS'), 'Port' (all set to '1812'), 'Shared Secret' (all masked with 'XXXXXXXXXX'), 'Retran Int (sec)' (all set to '5'), and 'Max Retran' (all set to '3'). Below each row is a 'Use server for:' section with checkboxes for 'EAP Authentication' (checked), 'MAC Address Authentication', 'User Authentication', and 'MIP Authentication'. A note at the bottom states: 'Note: For each authentication function, the most recently used server is shown in green text.' At the bottom right are buttons for 'Apply', 'OK', 'Cancel', and 'Restore Defaults'. A small number '65555' is visible in the bottom right corner of the form area.

You can configure up to four servers for authentication services, so you can set up backup authenticators. If you set up more than one server for the same service, the server first in the list is the primary server for that service, and the others are used in list order when the previous server times out.

- Step 7** Enter the name or IP address of the authentication server in the Server Name/IP entry field.


- Step 8** Enter the port number the server uses for authentication. The default setting, *1812*, is the port setting for Cisco's RADIUS server, the Cisco Secure Access Control Server (ACS), and for many other RADIUS servers. Check your server's product documentation to find the correct port setting.
- Step 9** Enter the shared secret used by the server in the Shared Secret entry field. The shared secret on the bridge must match the shared secret on the server.
- Step 10** Enter the number of seconds the access point should try contacting the primary authentication server in the Timeout entry field. If the primary authentication server does not respond within this time, the access point tries to contact the backup authentication server if one is specified.
- Step 11** Select **MAC Address Authentication** under the server. If you set up a backup authentication server, select **MAC Address Authentication** under the backup server, also.
- Step 12** Click **OK**. You return automatically to the Setup page.
- Step 13** Create a list of allowed MAC addresses for your authentication server. Enter the MAC addresses of all allowed clients as users in the server's database. The "Enabling MAC-Based Authentication in Cisco Secure ACS" section on page 8-35 describes how to create a list of MAC addresses for your RADIUS server.
-  **Note** Be sure to include your own MAC address in the authentication server's list.
- Step 14** Click **Advanced** in the AP Radio row of the Network Ports section at the bottom of the Setup page. The AP Radio Advanced page appears. Figure 8-12 shows the AP Radio Advanced page.

Figure 8-12 AP Radio Advanced Page

Map Help Uptime: 3 days, 17:01:17

Requested Status: Up

Current Status: Up

Packet Forwarding: Enabled

Forwarding State: Forwarding

Default Multicast Address Filter: Allowed

Maximum Multicast Packets/Second: 0

Radio Cell Role: Access Point/Root

SSID for use by Infrastructure Stations (such as Repeaters): 0

Disallow Infrastructure Stations on any other SSID: ☐ yes ☒ no

Use Aironet Extensions: ☒ yes ☐ no

Classify Workgroup Bridges as Network Infrastructure: ☒ yes ☐ no

Require use of Radio Firmware 4.99H: ☒ yes ☐ no

Ethernet Encapsulation Transform: RFC1042

Quality of Service Setup

If VLANs are *not* enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through VLAN Setup.

Enhanced MIC verification for WEP: None

Temporal Key Integrity Protocol: None

Broadcast WEP Key rotation interval (sec): 0 (0=off)

To configure 802.11 Authentication, EAP, Unicast Address Filters, and the Maximum Number of Associations for this radio's Primary SSID (the default SSID), please use the link below.

Advanced Primary SSID Setup

Specified Access Point 1: 00:00:00:00:00:00

Specified Access Point 2: 00:00:00:00:00:00

Specified Access Point 3: 00:00:00:00:00:00

Specified Access Point 4: 00:00:00:00:00:00

Radio Modulation: Standard

Radio Preamble: Short

Apply OK Cancel Restore Defaults

Step 15 Select **Disallowed** from the pull-down menu for Default Unicast Address Filter for each authentication type requiring MAC-based authentication.

For example, if the access point is configured for both open and Network-EAP authentication, you could set Default Unicast Address Filter under Open to Disallowed but leave Default Unicast Address Filter under Network-EAP set to Allowed. This configuration forces client devices using open authentication to authenticate using MAC addresses but does not force LEAP-enabled client

devices to authenticate using MAC addresses. To force all client devices to authenticate using MAC addresses, select **Disallowed** for all the enabled authentication types.

When you set Default Unicast Address Filter to disallowed, the access point discards all unicast traffic except packets sent to the MAC addresses listed as allowed on the authentication server or on the access point's Address Filters page.



Note Client devices associated to the access point are not immediately affected when you set Default Unicast Address Filter to disallowed.

- Step 16** Click **OK**. You return automatically to the Setup page. Client devices that associate with the access point will not be allowed to authenticate unless their MAC addresses are included in the list of allowed addresses.
-

Authenticating Client Devices Using MAC Addresses or EAP

You can set up the access point to authenticate client devices using a combination of MAC-based and EAP authentication. When you enable this feature, client devices that associate to the access point using 802.11 open authentication first attempt MAC authentication. If MAC authentication succeeds, the client device joins the network; if the client is also using EAP authentication, it attempts to authenticate using EAP. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication.

Follow these steps to combine MAC-based and EAP authentication for client devices using 802.11 open authentication:

-
- Step 1** Follow the steps in the “Setting Up EAP Authentication” section on page 8-20 to set up EAP. You must select **Require EAP** under Open authentication on the AP Radio Data Encryption page to force client devices to perform EAP authentication if they fail MAC authentication. If you do not select **Require EAP**, client devices that fail MAC authentication might be able to join the network without performing EAP authentication.
- Step 2** Follow the steps in the “Setting Up MAC-Based Authentication” section on page 8-29 to set up MAC-based authentication.

- Step 3** Follow this link path to reach the Address Filters page:
- On the Summary Status page, click **Setup**.
 - On the Setup page, click **Address Filters** under Associations.
- Step 4** Select **yes** for the option called *Is MAC Authentication alone sufficient for a client to be fully authenticated?*
- Step 5** Click **Apply**. When you enable this feature, the access point follows these steps to authenticate all clients that associate using 802.11 open authentication:
- When a client device sends an authentication request to the access point, the access point sends a MAC authentication request in the RADIUS Access Request Packet to the RADIUS server using the client's user ID and password as the MAC address of the client.
 - If the authentication succeeds, the client joins the network. If the client is also using EAP authentication, it attempts to authenticate using EAP.
 - If MAC authentication fails for the client, the access point allows the client to attempt to authenticate using EAP authentication. The client cannot join the network until EAP authentication succeeds.
-

Enabling MAC-Based Authentication in Cisco Secure ACS

Cisco Secure Access Control Server for Windows NT/2000 Servers (Cisco Secure ACS) can authenticate MAC addresses sent from the access point. The access point works with ACS to authenticate MAC addresses using Secure Password Authentication Protocol (Secure PAP). You enter a list of approved MAC addresses into the ACS as users, using the client devices' MAC addresses as both the username and password. The authentication server's list of allowed MAC addresses can reside on the authentication server or at any network location to which the server has access.

Follow these steps to create a list of allowed MAC addresses in Cisco Secure ACS:

-
- Step 1** On the ACS main menu, click **User Setup**.
- Step 2** When the User text box appears, enter the MAC address you want to add to the list.

**Note**

The access point sends MAC address queries to the server using lower-case characters. If your server allows case-sensitive usernames and passwords, you must enter MAC addresses in the server's database using lower-case characters.

- Step 3** When the User Setup screen appears, enter the MAC address in the Cisco Secure PAP Password and Confirm Password entry fields.
- Step 4** Enter the MAC address in the CHAP/MS-CHAP/ARAP Password and Confirm Password entry fields.
- Step 5** Select the Separate (CHAP/MS-CHAP/ARAP) checkbox.
- Step 6** Click **Submit**. Repeat these steps for each MAC address you want to add to the list of allowed MAC addresses.

MAC addresses that you enter in the authentication server's list appear in the access point's address filter list when the client device is associated to the access point. MAC addresses in the server's list disappear from the access point's list when the client devices disassociate or when the access point is reset.

**Note**

Be sure to include your own MAC address in the authentication server's list to avoid losing connectivity to the access point.

Summary of Settings for Authentication Types

Table 8-5 lists the access point settings required to enable each authentication type and combinations of authentication types.

Table 8-5 *Settings for Authentication Types*

Authentication Types	Required Settings
LEAP	<p>On the Authenticator Configuration page (shown in Figure 8-13):</p> <ul style="list-style-type: none">• Select an 802.1X protocol draft that matches the protocol draft used by client devices that associate with the access point.• Enter the name or IP address, type, port, shared secret, and timeout value for your RADIUS server.• Select the EAP checkbox under the server. <p>On the AP Radio Data Encryption page (shown in Figure 8-6):</p> <ul style="list-style-type: none">• Select the Network-EAP checkbox.• Enter a WEP key in key slot 1 and select 128-bit from the key size menu.
LEAP and static WEP under 802.11 Open	<ul style="list-style-type: none">• Enter all the settings for LEAP authentication. <p>On the AP Radio Data Encryption page (shown in Figure 8-6):</p> <ul style="list-style-type: none">• Select the Open checkbox.

Table 8-5 Settings for Authentication Types (continued)

Authentication Types	Required Settings
EAP-TLS and EAP-MD5	<p>On the Authenticator Configuration page (shown in Figure 8-13):</p> <ul style="list-style-type: none"> • Select an 802.1X protocol draft that matches the protocol draft used by client devices that associate with the access point. • Enter the name or IP address, type, port, shared secret, and timeout value for your RADIUS server. • Select the EAP checkbox under the server. <p>On the AP Radio Data Encryption page (shown in Figure 8-6):</p> <ul style="list-style-type: none"> • Select the Open and Network-EAP checkboxes. • Select the Require EAP checkbox under Open. <p>Note Selecting Require EAP blocks non-EAP client devices from using the access point.</p> <ul style="list-style-type: none"> • Enter a WEP key in key slot 1 and select 128-bit from the key size pull-down menu.
EAP-TLS, EAP-MD5, and static WEP under 802.11 Open	<p>The access point does not support this combination of authentication types. When you select Require EAP on the Authenticator Configuration page to authenticate clients using EAP-TLS and EAP-MD5, non-EAP client devices are blocked from using the access point. However, the access point can serve client devices using 802.11 open authentication if the access point is set up for MAC-based authentication and EAP authentication. See the “Authenticating Client Devices Using MAC Addresses or EAP” section on page 8-34 for instructions on setting up this combination of authentications.</p>

Table 8-5 Settings for Authentication Types (continued)

Authentication Types	Required Settings
MAC-based	<p>On the Address Filters page (shown in Figure 8-10):</p> <ul style="list-style-type: none"> Select yes for the “Look up MAC address on authentication server if not in existing filter list” setting. <p>On the Authenticator Configuration page (shown in Figure 8-13):</p> <ul style="list-style-type: none"> Select an 802.1X protocol draft that matches the protocol draft used by client devices that associate with the access point. Enter the name or IP address, type, port, shared secret, and timeout value for your RADIUS server. Select the MAC Address Authentication checkbox under the server. <p>Note You can use the same server for both EAP authentication and MAC-based authentication.</p> <p>On the AP Radio Advanced page (shown in Figure 8-12):</p> <ul style="list-style-type: none"> Select Disallowed from the pull-down menu for Default Unicast Address Filter for each authentication type requiring MAC-based authentication.
MAC-based and EAP-TLS and EAP-MD5	<ul style="list-style-type: none"> Enter the settings for the EAP authentication types you need to support; select Require EAP on the AP Radio Data Encryption page under Open. Enter the settings for MAC-based authentication. <p>On the Address Filters page (shown in Figure 8-10):</p> <ul style="list-style-type: none"> Select yes for the setting called “Is MAC Authentication alone sufficient for a client to be fully authenticated?”
MAC-based and LEAP	<ul style="list-style-type: none"> Enter the settings for LEAP. Enter the settings for MAC-based authentication.

Setting Up Backup Authentication Servers

You can configure up to four servers for authentication services on the Authenticator Configuration page, so you can set up backup authenticators. If you set up more than one server for the same service, the server first in the list is the primary server for that service, and the other servers are used in list order when the previous server times out. If a backup server responds after the primary server fails, the access point continues to use the backup server for new transactions.

Follow these steps to set up a backup authentication server:

-
- Step 1** Complete the steps in the “Setting Up EAP Authentication” section on page 8-20 or the “Setting Up MAC-Based Authentication” section on page 8-29 to set up your primary authentication server.
- Step 2** On the Authenticator Configuration page, enter information about your backup server in one of the entry field groups under the completed entry fields for your primary server:
- a. Enter the name or IP address of the backup server in the Server Name/IP entry field.
 - b. Enter the port number the server uses for authentication. The default setting, *1812*, is the port setting for Cisco’s RADIUS server, the Cisco Secure Access Control Server (ACS), and for many other RADIUS servers. Check your server’s product documentation to find the correct port setting.
 - c. Enter the shared secret used by the server in the Shared Secret entry field. The shared secret on the bridge must match the shared secret on the server.
 - d. Enter the number of seconds the the access point should wait before authentication fails.
 - e. Enter the number of seconds the access point should wait before giving up contacting the server.
- Step 3** Select the same authentication methods as those selected on the primary server.
- Step 4** Click **OK**. You return automatically to the Setup page. Figure 8-13 shows a primary authentication server and a backup server configured on the Authenticator Configuration page.

Figure 8-13 Authenticator Configuration Page with Primary and Backup Servers

Map

Help

Uptime: 1 day, 19:55:08

802.1X Protocol Version (for EAP Authentication):

802.1x-2001

Primary Server Reattempt Period (Min.):

0

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran
	RADIUS	1812		5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
	RADIUS	1812		5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
	RADIUS	1812		5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
	RADIUS	1812		5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					

Note: For each authentication function, the most recently used server is shown in green text.

Apply

OK

Cancel

Restore Defaults

65556

Setting Up Administrator Authorization

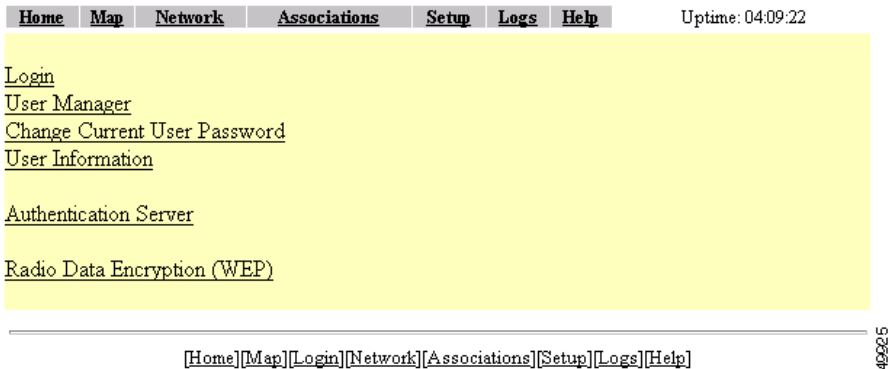
Administrator authorization protects the access point management system from unauthorized access. Use the access point's user management pages to define a list of users who are authorized to view and change the access point management system. Use the Security Setup page to reach the user management pages. Figure 8-14 shows the Security Setup page.



Note

Creating a list of users authorized to view and change the access point management system does not affect the ability of client devices to associate with the access point.

Figure 8-14 Security Setup Page



Follow this link path to reach the Security Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Security**.

Creating a List of Authorized Management System Users

Follow these steps to create a list of users authorized to view and change the access point management system:

- Step 1** Follow the link path to the Security Setup page.
- Step 2** On the Security Setup page, click **User Information**. Figure 8-15 shows the User Information page.

Figure 8-15 User Information Page

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 4 days, 22:35:25
User Name		Write	SNMP	Ident	Firmware	Admin	
JaneDoe		x	x			x	
JoeSmith		x		x	x	x	
Add New User							

- Step 3** Click **Add New User**. The User Management window appears. Figure 8-16 shows the User Management window.

Figure 8-16 User Management Window

- Step 4** Enter a username and password for the new user.

- Step 5** Select the capabilities you want to assign to the new user. Capabilities include:

- **Write**—The user can change system settings. When you assign Write capability to a user, the user also automatically receives Admin capability.
- **SNMP**—Designates the username as an SNMP community name. SNMP management stations can use this SNMP community name to perform SNMP operations. The User Manager does not have to be enabled for SNMP communities to operate correctly.



Note

Selecting the SNMP checkbox does not grant SNMP write capability to the user; it only designates the username as an SNMP community name. SNMP operations performed under the username are restricted according to the username's other assigned capabilities.

- **Ident**—The user can change the access point's identity settings (IP address and SSID). When you assign Ident capability to a user, the user also automatically receives Write and Admin capabilities.

- **Firmware**—The user can update the access point's firmware. When you assign Firmware capability to a user, the user also automatically receives Write and Admin capabilities.
- **Admin**—The user can view most system screens. To allow the user to view all system screens and make changes to the system, select Write capability.

Step 6 Click **Apply**. The User Management window disappears, and the new user appears in the user list on the User Information page.

Step 7 Click the browser's **Back** button to return to the Security Setup page. On the Security Setup page, click **User Manager**. The User Manager Setup page appears. Figure 8-17 shows the User Manager Setup page.

Figure 8-17 User Manager Setup Page

Map Help Uptime: 01:42:02

User Manager: ☐ Enabled ☒ Disabled

Allow Read-Only Browsing without Login? ☒ yes ☐ no

Protect Legal Credit Page? ☐ yes ☒ no

Apply OK Cancel Restore Defaults

Step 8 Select **User Manager: Enabled** to restrict use of the access point management system to users in the user list.



Note

You must define a full administrator user—a user with write, identity, and firmware capabilities—before you can enable the user manager.

Use the other settings on the User Manager Setup page to add more restrictions for the management system:

- **Allow Read-Only Browsing without Login**—Select **yes** to allow any user to view the access point's basic screens. Select **no** to restrict access to all of the access point's screens to only the users in the user list.

- **Protect Legal Credit Page**—Select **yes** to restrict access to the Legal Credits page to users in the user list. Select **no** to allow any user to view the Legal Credits page.

Step 9 Click **OK**. You return automatically to the Security Setup page.

Setting up Centralized Administrator Authentication

The Centralized Administrator Authentication feature on the access point allows the use of an AAA server (RADIUS or TACACS) services to authenticate users when the User Manager function is enabled on the access point. The AAA server verifies the user login and passes back the appropriate privileges for the user (or administrator) when a login attempt is successful.



Note

You must have at least one user configured on the access point before you can enable the user manager feature.

Follow these steps to set up Centralized Administrator Authentication on the access point.

- Step 1** From Services section of the Setup page, click **Security**. The Security Setup page appears.
- Step 2** Click **User Information**. The User Information page appears.
- Step 3** Click **Add New User**. The User Management window appears.
- Step 4** Add a new user with full administrative capabilities (all capability settings checked).
- Step 5** Click **Apply**. You are returned to the User Information page.
- Step 6** Click **Back**. You are returned to the Security Setup page.
- Step 7** Click **User Manager**. The User Manager Setup page appears.
- Step 8** Enable User Manager and click **OK**. You are returned to the Security Setup page.
- Step 9** Click **Authentication Server**. The Authenticator Configuration page appears. See Figure 8-18.

Map
Help

Uptime: 1 day, 19:55:08

802.1X Protocol Version (for EAP Authentication):
802.1x-2001

Primary Server Reattempt Period (Min.):
0

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran
	RADIUS	1812	XXXXXXXXXXXXXXXX	5	3
Use server for:	<input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication	<input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication			
	RADIUS	1812	XXXXXXXXXXXXXXXX	5	3
Use server for:	<input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication	<input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication			
	RADIUS	1812	XXXXXXXXXXXXXXXX	5	3
Use server for:	<input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication	<input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication			
	RADIUS	1812	XXXXXXXXXXXXXXXX	5	3
Use server for:	<input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication	<input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication			

Note: For each authentication function, the most recently used server is shown in green text.

Apply
OK
Cancel
Restore Defaults

- a. Assign an IP address or name in the Server Name/IP field.
- b. Select the server type your network is using, either RADIUS or TACACS.
- c. Assign a port number for the server.



The default port settings are 1812 for RADIUS servers and 49 for TACACS servers. Check your server's product documentation for the correct port setting.

- d. Enter the shared secret used by your RADIUS or TACACS server in the Shared Secret entry field. The shared secret can contain up to 64 alphanumeric characters.
- e. Enter the number of seconds the access point should wait before it attempts to contact the server after a failed attempt.
- f. Enter the number of times the access point should attempt to contact the server before authentication fails in the Max Retran field.
- g. Select **User Authentication** in the Use server for line.
- h. Click **Apply** or **OK** to save your settings.

Step 11 Configure other servers as required.



Network Management

This section describes how to browse to other devices on your network, how to use Cisco Discovery Protocol with your wireless networking equipment, how to assign a specific network port to a MAC address, and how to enable wireless network accounting.

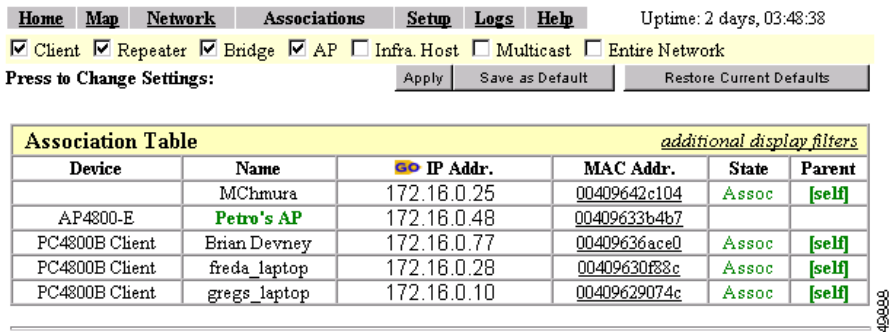
This chapter contains the following sections:

- Using the Association Table, page 9-2
- Using the Network Map Window, page 9-11
- Using Cisco Discovery Protocol, page 9-12
- Assigning Network Ports, page 9-13
- Enabling Wireless Network Accounting, page 9-15

Using the Association Table

The management system’s Association Table page lists all the devices, both wireless and wired to the root LAN, of which the access point is aware. Figure 9-1 shows an example of the Association Table page.

Figure 9-1 Association Table Page



Click the **Association** link at the top of any main management system page to go to the Association Table.



Note

You can also use the Association Table page in the command-line interface.

Browsing to Network Devices

To browse to a device’s browser-based interface, click the device’s IP address in the IP Addr. column. The home page of the device’s management system appears. Cisco Aironet access points, bridges, and workgroup bridges have browser-based interfaces, and many servers and printers have them, also.

If the device does not have a browser-based interface, click the device’s MAC address in the MAC Addr. column. A Station page appears for the device, displaying the information the access point knows about the device, including the device’s identity and statistics on traffic to and from the device. Some devices, such as PC card client adapters, do not have browser-based interfaces.

Setting the Display Options

You use the display options to select the device types to be listed in the table. The default selections list only the access point and any devices with which it is associated. To change the selections, click a display option and then click **Apply**.

To modify the table further, click **additional display filters**, which is a link to the Association Table Filters page. You use the Association Table Filters page to select the columns of information that appear in the Association Table and the order in which devices are listed.

For more information on customizing the Association Table display, read the “Association Table Display Setup” section on page 7-13.

Using Station Pages

Click a device’s MAC address in the Association Table’s MAC Addr. column to display a Station page for the device.


Station pages provide an overview of a network device’s status and data traffic history. The information on a Station page depends on the device type; a Station page for an access point, for example, contains different information than the Station page for a PC card client adapter.

You can also use the Station page to perform pings and link tests for network devices. Figure 9-2 shows a sample Station page for a PC card client adapter.

Figure 9-2 Station Page

HomeMapNetworkAssociationsSetupLogsHelp

Uptime: 18 days, 16:47:59

System Name	AP350-478916	Device	350 Series AP
MAC Address	[Aironet]00:40:96:47:89:16		
IP Address	 192.168.147.47		
VLAN ID	0	Policy Grp.	0
State	[self]	Class	Access Point
Status	OK		

Clear StatsRefresh

Number of Pkts. 5Pkt. Size 64Ping

To StationAlert <input type="checkbox"/>		From StationAlert <input type="checkbox"/>	
Packets OK	49476	Packets OK	185183
Total Bytes OK	8811286	Total Bytes OK	18884748
Total Errors	0	Total Errors	0
Max. Retry Pkts.	0		
Short Retries	0	WEP Errors	0
Long Retries	0		

Stations Associated	0 Clients, 0 Repeaters, 0 Bridges		
Load	0	Software Version	12.00
Uptime	18 days, 16:47:55	Announcement Pkts.	107710

Hops to Infra.	0	Echo Packets	0
Activity Timeout	never	Latest Activity	00:00:00
Communication Over Interface: Ethernet fec0			

49926

Information on Station Pages

Station Identification and Status

- The yellow table at the top of the Station page lists the following information:
- System Name—The name assigned to the device.
 - Device—The type and model number of the device.
 - MAC Address—A unique identifier assigned by the manufacturer.

- IP Address—The device's IP address.

When you click the IP address link, the browser attempts to display the device's home page. Cisco Aironet access points, bridges, and workgroup bridges have browser-based interfaces, and many servers and printers have them also.

- VLAN ID—The identification number of configured VLANs.

Policy Grp.—A group of filters specifically designed to allow or deny certain types of traffic to or from the access point.

- State—Displays the operational state of the wireless station. Possible states include:
 - Assoc—The station is associated with an access point. Client stations associated with this access point will also show an Association Identifier (AID) value that is an index into a table of stations associated with this access point. Maximum AID count is 2007.
 - Unauth—The station is not authenticated with any access point.
 - Auth—The station is authenticated with an access point.
 - Local Auth—The station has authenticated at least once with this access point.
- Class—This field displays the type of station. Station types include:
 - AP—An access point.
 - Client, PS Client—A client or power-save client station.
 - Bridge, Bridge R—A bridge or a root bridge.
 - Rptr—A repeater.
 - Mcast—A multicast address.
 - Infra—An infrastructure node, typically a workstation with a wired connection to the Ethernet network.
- Status—This field indicates the device's operating status. Possible statuses include:
 - OK—The device is operating properly.
 - EAP Pending
 - EAP Autenticated
 - IP Forwarding Agent

- BootP/DHCP Client—The device is using BOOTP or DHCP protocol
- ARP Proxy Server
- IP Virtual Router
- WEP—WEP is enabled on the device.

To Station Information

Fields in the To Station column in the second table on the Station page contain the following information:

- Alert—Click this box if you want detailed packet trace information captured for the Association Table page. This option is only available to users with Administrator capability.
- Packets OK—Reports the number of good packets coming to the station.
- Total Bytes OK—Reports the number of good bytes coming to the station.
- Total Errors—Reports the total number of packet errors coming to the station.
- Max. Retry Pkts.—Reports the number of times data packets have reached the maximum long or short retry number. Set the maximum RTS value on the AP Radio Hardware page; see the “Entering Radio Hardware Information” section on page 3-11 for instructions.
- RTS (Short) Retries—Reports the number of times the RTS packet had to be retried.
- Data (Long) Retries—Reports the number of times the data packet had to be retried.

From Station Information

Fields in the To Station column contain the following information:

- Alert—Click this box if you want detailed packet trace information captured for the Association Table page. This option is only available to users with Administrator capability.
- Packets OK—Reports the number of good packets sent from the station.
- Total Bytes OK—Reports the number of good bytes sent from the station.
- Total Errors—Reports the total number of packet errors sent from the station.
- WEP Errors—Reports the number of encryption errors sent from the station.

Rate, Signal, and Status Information

The table under the To and From Station table lists rate, signal, and status information for the device.

Data rate and signal quality information appears on Station pages for client devices. On Station pages for access points, this area shows network information such as system uptime.

- **Parent**—Displays the system name of the device to which the client, bridge or repeater is associated. The entry [self] indicates that the device is associated with this access point.
- **Current Rate**—Reports the current data transmission rate. If the station is having difficulty communicating with the access point, this might not be the highest operational rate.
- **Latest Retries**—Tally of short and long data retries.
- **Next Hop**—If repeater access points are used on the network, this field names the next access point in the repeater chain.
- **Operational Rates**—The data transmission rates in common between the access point and the station.
- **Latest Signal Strength**—Displays the current index of radio signal quality.

The following four fields appear only on the Station page for an access point:

- **Stations Associated**—Displays, by number and class, all stations associated with the access point.
- **Uptime**—Displays the cumulative time the device has been operating since the last reset.
- **Software Version**—Displays the version level of Cisco software on the device.
- **Announcement Packets**—Total number of Announcement packets since the device was last reset.

Hops and Timing Information

The table at the bottom of the Station page lists information on the chain of devices, if any, between the device and the wired LAN, on the monitoring timeout for the device, and on the time of the most recent system activity.

- Hops to Infra.—The number of devices between this station and the network infrastructure.
- Activity Timeout—Total time that can elapse after the access point's last data receipt before the access point presumes the client device has been turned off. See the “Using the Association Table” section on page 9-2 for information on setting timeouts for each device class.
- Communication Over Interface—The network port over which the access point or bridge is communicating with the device.
- Echo Packets—The link test sequence number; it lists the total number of link test packets sent to this station.
- Latest Activity—Elapsed time in hours, minutes, and seconds since the station and the access point last communicated. All zeros means there is current communication.

Performing Pings and Link Tests

Use the ping and link test buttons to perform pings and link tests on the device. If the device is associated to the access point through which you reached the Station page, the link test button and packet fields appear. If the device is not associated with the access point, only the ping button and packet fields appear.

Performing a Ping

Follow these steps to ping the device described on the Station page:

-
- Step 1** To customize the size and number of packets sent during the ping, enter the number of packets and size of the packets in the Number of Pkts. and Pkt. Size fields.
- Step 2** Click **Ping**.
- The ping runs using the values in the Number of Pkts. and Pkt. Size fields, and a ping window appears listing the test results. To run the ping again, click **Test Again**. Figure 9-3 shows a ping window.

Figure 9-3 Ping Window

```
PING 161.44.236.219: 56 data bytes
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=2. time<19 msec
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=3. time<19 msec
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=4. time<19 msec
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=5. time<19 msec
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=6. time<19 msec
----161.44.236.219 PING Statistics----
7 packets transmitted, 5 packets received, 28% packet loss
round-trip (ms)  min/avg/max = 0/0/0
```

Test Again

49923

Performing a Link Test

Follow these steps to perform a link test between the access point and the device described on the Station page:

Step 1 To customize the size and number of packets sent during the link test, enter the number of packets and size of the packets in the Number of Pkts. and Pkt. Size fields.

Step 2 Click **Link Test**.

The link test runs using the values in the Number of Pkts. and Pkt. Size fields.



Note If you need to stop the link test before the test is complete, click **Stop Test**.

A results window appears listing the test results. To run the test again, click **Test Again**. To run a continuous link test, click **Continuous Test**. Figure 9-4 shows a link test results window.

Figure 9-4 Link Test Results Window

Pkts. Attempted	100	Pkts. Requested	100
Pkts. Successful	100	Payload Size	500
Avg. Delay	19.2 msec	[Min, Max] Delay	[19.2, 19.2] msec
Transmit Rates	100 at 11.0B		

To the Station		From the Station	
Avg. Signal Strength	96%	Avg. Signal Strength	84%
[Min, Max] Strength	[80%, 100%]	[Min, Max] Strength	[70%, 100%]
Pkts. No Retries	95	Pkts. No Retries	96
Pkts. 1 Retry	5	Pkts. 1 Retry	4
Pkts. Mult. Retries	0	Pkts. Mult. Retries	0
Pkts. Max. Retries	0		
Pkts. Lost	0	Pkts. Lost	0
Duplicate Pkts.	0	Duplicate Pkts.	0
RTS Retries	0	RTS Retries	0
Data Retries	5	Data Retries	4

Test Again Continuous Test

49360

Clearing and Updating Statistics

Use the Clear Stats and Refresh buttons to clear and update the Station page statistics.

- Clear Stats—Clears all packet, octet and error counts and resets the counters to 0.
- Refresh—Updates the counts to their latest accumulated values, and saves the Alert selections.

Deauthenticating and Disassociating Client Devices

Use the Deauthenticate and Disassociate buttons to deauthenticate and disassociate the client device from the access point. These buttons appear only on Station pages for devices that are associated with the access point, and only users with administrator capability can operate them.

- Deauthenticate—Forces a client to re-authenticate with the access point.

- **Disassociate**—Allows a client to break its current association, re-evaluate the currently associated access point and determine which of the surrounding access points has the best signal quality to associate with.

Using the Network Map Window

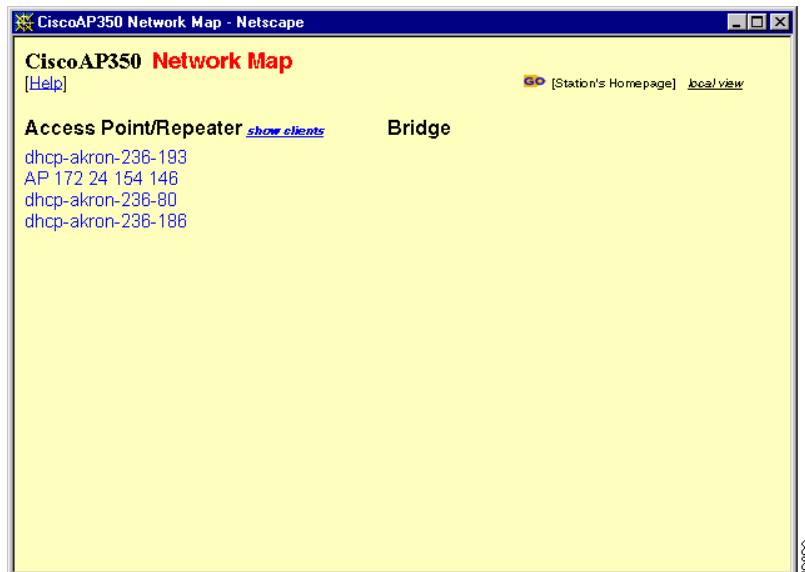
To open the Network Map window, click **Map** at the top of any management system page. (See the “Using the Network Map Window” section on page 9-11 for information about the Map page.) When the Map window appears, click **Network Map**.

You use the Network Map window to open a new browser window displaying information for any device on your wireless network. Unlike the Association Table, the Network Map window does not list wired devices on your LAN. Figure 9-5 shows the Network Map window.

**Note**

Your Internet browser must have Java enabled to use the map windows.

Figure 9-5 Network Map Window



Click the name of a wireless device to open a new browser window displaying a Station page displaying the access point's local information for that device. Click **Go** beside the device name to open a new browser window displaying that device's home page, if available. Some devices, such as PC card clients, do not have browser-based interfaces.

Click **show clients** to display all the wireless client devices on your network. The client names appear under the access point or bridge with which they are associated. If clients are displayed, click **hide clients** to display only non-client devices.

Using Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices. Information in CDP packets is used in network management software such as CiscoWorks2000.

Use the CDP Setup page to adjust the access point's CDP settings. CDP is enabled by default. Figure 9-6 shows the CDP Setup page.

Figure 9-6 CDP Setup Page

Map Help Uptime: 1 day, 06:48:18

Cisco Discovery Protocol (CDP): ☒ Enabled ☐ Disabled

Packet hold time: 180 Seconds

Packets sent every: 60 Seconds

Individual Interface Enable:

☒ 01: Ethernet

Apply OK Cancel Restore Defaults

Follow this link path to reach the CDP Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services**.

3. On the Cisco Services Setup page, click **Cisco Discovery Protocol (CDP)**.

Settings on the CDP Setup Page

The CDP Setup page contains the following settings:

- Enabled/Disabled—Select **Disabled** to disable CDP on the access point; select **Enabled** to enable CDP on the access point. CDP is enabled by default.
- Packet hold time—The number of seconds other CDP-enabled devices should consider the access point's CDP information valid. If other devices do not receive another CDP packet from the access point before this time elapses they should assume that the access point has gone offline. The default value is 180. The packet hold time should always be greater than the value in the "Packets sent every" field.
- Packets sent every—The number of seconds between each CDP packet the access point sends. The default value is 60. This value should always be less than the packet hold time.
- Individual Interface Enable: Ethernet—When selected, the access point sends CDP packets through its Ethernet port and monitors the Ethernet for CDP packets from other devices.

MIB for CDP

A MIB file is available for use with CDP. The filename is CISCO-CDP-MIB.my, and you can download the MIB at the following URL:

<http://www.cisco.com/public/mibs>

Assigning Network Ports

Use the Port Assignments page to assign a specific network port to a repeater access point or to a non-root bridge. When you assign specific ports, your network topology remains constant even when devices reboot. Figure 9-7 shows the Port Assignments page.

Figure 9-7 Port Assignments Page

MapHelp

2001/07/16 14:09:02

ifIndex	dot1dBasePort	AID	Station
10	6	2	00:00:00:00:00:00
11	7	3	00:00:00:00:00:00
12	8	4	00:00:00:00:00:00
13	9	5	00:00:00:00:00:00
14	10	6	00:00:00:00:00:00
15	11	7	00:00:00:00:00:00
16	12	8	00:00:00:00:00:00
17	13	9	00:00:00:00:00:00
18	14	10	00:00:00:00:00:00
19	15	11	00:00:00:00:00:00
20	16	12	00:00:00:00:00:00
21	17	13	00:00:00:00:00:00
22	18	14	00:00:00:00:00:00
23	19	15	00:00:00:00:00:00
24	20	16	00:00:00:00:00:00
25	21	17	00:00:00:00:00:00
26	22	18	00:00:00:00:00:00
27	23	19	00:00:00:00:00:00
28	24	20	00:00:00:00:00:00
29	25	21	00:00:00:00:00:00
30	26	22	00:00:00:00:00:00
31	27	23	00:00:00:00:00:00
32	28	24	00:00:00:00:00:00
33	29	25	00:00:00:00:00:00
34	30	26	00:00:00:00:00:00
35	31	27	00:00:00:00:00:00
36	32	28	00:00:00:00:00:00

ApplyOKCancelRestore Defaults

50662

Follow this link path to reach the Port Assignments page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Port Assignments** in the Association section near the top of the page.

Settings on the Port Assignments Page

- ifIndex—Lists the port's designator in the Standard MIB-II (RFC1213-MIB.my) interface index.
- dot1dBasePort—Lists the port's designator in the Bridge MIB (RFC1493; BRIDGE-MIB.my) interface index.
- AID—Lists the port's 802.11 radio drivers association identifier.
- Station—Enter the MAC address of the device to which you want to assign the port in the port's Station entry field. When you click **Apply** or **OK**, the port is reserved for that MAC address.

Enabling Wireless Network Accounting

You can enable accounting on the access point to send network accounting information about wireless client devices to a RADIUS server on your network. Cisco Secure ACS writes accounting records to a log file or to a database daily. Consult the *Cisco Secure ACS 2.6 for Windows 2000/NT Servers User Guide* for instructions on viewing and downloading the log or database:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/csnt26/index.htm

If you have a UNIX server, use this URL to browse to the *CiscoSecure ACS 2.3 for UNIX User Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx/csu23ug/index.htm



Note

RADIUS accounting is available in firmware versions 11.10T and later, which are available on Cisco.com. You can download Cisco Aironet firmware releases at <http://www.cisco.com/public/sw-center/sw-wireless.shtml>.

Use the Accounting Setup page to enable and set up accounting on the access point. Figure 9-8 shows the Accounting Setup page.

Figure 9-8 Accounting Setup Page

[Map](#)
[Help](#)

Uptime: 1 day, 22:30:15

Enable accounting:

☐ Enabled
 ☒ Disabled

Enable delaying to report STOP:

☒ Enabled
 ☐ Disabled

Minimum delay time to report STOP (sec):

2

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran	Enable Update	Update Delay (sec)
	RADIUS	1813	AAAAAAAAAAAA	5	3	<input checked="" type="checkbox"/>	600
Use accounting server for: <input type="checkbox"/> EAP authentication <input type="checkbox"/> non-EAP authentication							
	RADIUS	1813	AAAAAAAAAAAA	5	3	<input checked="" type="checkbox"/>	600
Use accounting server for: <input type="checkbox"/> EAP authentication <input type="checkbox"/> non-EAP authentication							
	RADIUS	1813	AAAAAAAAAAAA	5	3	<input checked="" type="checkbox"/>	600
Use accounting server for: <input type="checkbox"/> EAP authentication <input type="checkbox"/> non-EAP authentication							
	RADIUS	1813	AAAAAAAAAAAA	5	3	<input checked="" type="checkbox"/>	600
Use accounting server for: <input type="checkbox"/> EAP authentication <input type="checkbox"/> non-EAP authentication							

Apply

OK

Cancel

Restore Defaults

65550

Follow this link path to reach the Accounting Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Accounting** under Services.

Settings on the Accounting Setup Page

The Accounting Setup page contains these settings:

- Enable accounting—Select Enabled to turn on accounting for your wireless network.
- Enable delaying to report stop—Select this option to delay sending a stop report to the server when a client device disassociates from the access point. The delay reduces accounting activity for client devices that disassociate from the access point and then quickly reassociate.

- **Minimum delay time to report stop (sec.)**—Enter the number of seconds the access point waits before sending a stop report to the server when a client device disassociates from the access point. The delay reduces accounting activity for client devices that disassociate from the access point and then quickly reassociate.
- **Server Name/IP**—Enter the name or IP address of the server to which the access point sends accounting data.
- **Server Type**—Select the server type from the pull-down menu. RADIUS is the only menu option; additional types will be added in future software releases.
- **Port**—The communication port setting used by the access point and the server. The default setting, 1813, is the correct setting for Cisco Aironet access points and Cisco secure ACS.
- **Shared Secret**—Enter the shared secret used by your RADIUS server. The shared secret on the device must match the shared secret on the RADIUS server.
- **Retran Int (sec.)**—Enter the number of seconds the access point should wait before giving up contacting the server. If the server does not respond within this time, the access point tries to contact the next accounting server in the list if one is specified. The access point uses backup servers in list order when the previous server times out.
- **Max Retran**—Enter the number of seconds the access point should wait before giving up contacting the server. If the server does not respond within this time, the access point tries to contact the next accounting server in the list if one is specified. The access point uses backup servers in list order when the previous server times out.
- **Enable Update**—Click the Enable Update checkbox to enable accounting update messages for wireless clients. With updates enabled, the access point sends an accounting start message when a wireless client associates to the access point, sends updates at regular intervals while the wireless client is associated to the access point, and sends an accounting stop message when the client disassociates from the access point. With updates disabled, the access point sends only accounting start and accounting stop messages to the server.
- **Update Delay**—Enter the update interval in seconds. If you use 360, the default setting, the access point sends an accounting update message for each associated client device every 6 minutes.

- Use accounting server for—Select the authentication types for which you want to collect accounting data. When you select **EAP authentication**, the access point sends accounting data to the server for client devices that authenticate using Cisco Aironet LEAP, EAP-TLS, or EAP-MD5. When you select **non-EAP authentication**, the access point sends data to the server for client devices using authentication types other than EAP, such as open, shared key, or MAC-based authentication.

Accounting Attributes

Table 9-1 lists the accounting attributes the access point sends to the accounting server.

Table 9-1 Accounting Attributes the Access Point Sends to the Accounting Server

Attribute	Definition
Acct-Status-Type	The client device’s current accounting status; possible statuses include ACCT_START, ACCT_STOP, and ACCT_UPDATE. The access point sends an ACCT_START frame to the accounting server when a client device successfully authenticates on a RADIUS server through the access point; the access point sends an ACCT_STOP frame to the server when a client device disassociates from the access point; and the access point sends an ACCT_UPDATE frame to the server periodically while the authenticated client device is associated to the access point.
Acct-Session-ID	A unique accounting identifier for each connection activity that is bounded by ACCT_START and ACCT_STOP. The access point sends this attribute to the server with all three status types.
User-Name	The username with which the client device’s authenticated to the network. The access point sends this attribute to the server with all three status types.

Table 9-1 *Accounting Attributes the Access Point Sends to the Accounting Server (continued)*

Attribute	Definition
NAS-Port	The port number used for the client device's connection. The access point sends this attribute to the server with all three status types.
Acct-Authentic	The method with which the client device is authenticated to the network. This value is always 1, which represents RADIUS authentication. The access point sends this attribute to the server with all three status types.
NAS-Identifier	The network access server (NAS) sending the accounting data; for wireless networks, the name of the access point sending the accounting information. The access point sends this attribute to the server with all three status types.
Acct-Session-Time	The elapsed time in seconds that the client device has been associated to the access point. The access point sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types.
Acct-Input-Octets	The number of octets received on the wireless network through the access point since the client device associated to the access point. The access point sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types.
Acct-Output-Octets	The number of octets sent on the wireless network through the access point since the client device associated to the access point. The access point sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types.
Acct-Input-Packets	The number of packets received on the wireless network through the access point since the client device associated to the access point. The access point sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types.

Table 9-1 *Accounting Attributes the Access Point Sends to the Accounting Server (continued)*

Attribute	Definition
Acct-Output-Packets	The number of packets sent on the wireless network through the access point since the client device associated to the access point. The access point sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types.
Acct-Terminate-Cause	How the client device's session was terminated. This attribute lists the same cause for every disassociated client device: Loss of service. The access point sends this attribute only with the ACCT_STOP status type.
Acct-Delay-Time	The delay between the time the event occurred and the time that the attribute was sent to the server. The access point sends this attribute to the server with all three status types.
RADIUS_IPADR	The IP address of the access point sending the accounting information. The access point sends this attribute to the server with all three status types.



Managing Firmware and Configurations

This section describes how to update the firmware version on the access point, how to distribute firmware to other access points, how to distribute the access point's configuration to other access points, and how to download, upload, and reset the access point configuration. You use the Cisco Services Setup page as a starting point for all these activities.

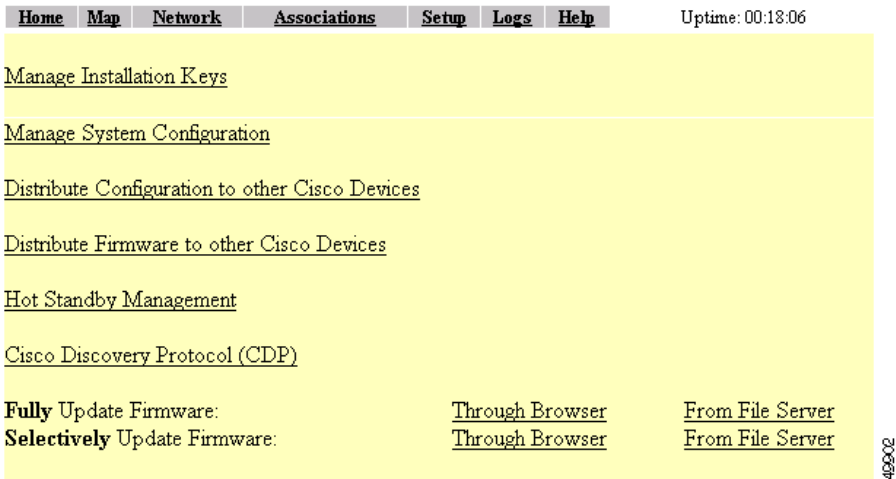
This chapter contains the following sections:

- Updating Firmware, page 10-2
- Distributing Firmware, page 10-9
- Distributing a Configuration, page 10-11
- Downloading, Uploading, and Resetting the Configuration, page 10-12

Updating Firmware

You use the Cisco Services Setup page to update the access point’s firmware. You can perform the update by browsing to a local drive or by using FTP to update the firmware from a file server. Figure 10-1 shows the Cisco Services Setup page.

Figure 10-1 Cisco Services Setup Page



Follow this link path in the browser interface to reach the Cisco Services Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.

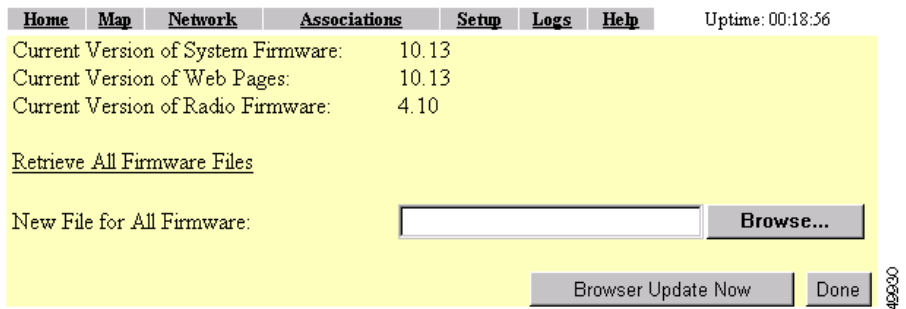
Updating with the Browser from a Local Drive

When you update the firmware with your browser, you browse to your hard drive or to a mapped network drive for the new firmware. You can update the three firmware components—the management system firmware, the firmware web pages, and the radio firmware—individually or all at once. It is simplest to update all the components at once, but in some situations you might want to update them individually.

Full Update of the Firmware Components

To update all the firmware components at the same time, click **Through Browser** on the Fully Update Firmware line on the Cisco Services Setup page. The Update All Firmware Through Browser page appears. Figure 10-2 shows the Update All Firmware Through Browser page.

Figure 10-2 Update All Firmware Through Browser Page



Follow these steps to update all three firmware components through the browser:

- Step 1** If you know the exact path and filename of the new firmware image file, type it in the New File for All Firmware entry field.
If you aren't sure of the exact path to the new firmware image file, click **Browse...** next to the New File entry field. When the File Upload window appears, go to the directory that contains the firmware image file and select the file. Click **Open**.
- Step 2** When the filename for the new firmware appears in the New File entry field, click **Browser Update Now** to load and install the new firmware. When the update is complete, the access point automatically reboots.

Selective Update of the Firmware Components

To update firmware components individually, click **Through Browser** on the Selectively Update Firmware line on the Cisco Services Setup page. The Update Firmware Through Browser page appears. Figure 10-3 shows the Update Firmware Through Browser page.

Figure 10-3 Update Firmware Through Browser Page

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 00:20:27
Current Version of System Firmware:			10.13				
Current Version of Web Pages:			10.13				
Current Version of Radio Firmware:			4.10				
New File for System Firmware:			<input type="text"/>		<input data-bbox="1085 618 1176 643" type="button" value="Browse..."/>		
New File for Web Pages:			<input type="text"/>		<input data-bbox="1085 656 1176 680" type="button" value="Browse..."/>		
New File for Radio Firmware:			<input type="text"/>		<input data-bbox="1085 693 1176 717" type="button" value="Browse..."/>		
					<input data-bbox="917 764 1096 789" type="button" value="Browser Update Now"/>		<input data-bbox="1161 764 1206 789" type="button" value="Done"/>

Follow these steps to update one of the three firmware components through the browser:

-
- Step 1** If you know the exact path and filename of the new firmware component, type it in the New File for [component] entry field.
- If you aren't sure of the exact path to the new component, click **Browse...** next to the component's New File entry field. When the File Upload window appears, go to the directory that contains the component and select the file. Click **Open**.
- Step 2** When the filename for the new component appears in the New File entry field, click **Browser Update Now** to load and install the new component. When the update is complete, the AP automatically reboots.
-

Updating from a File Server

When you update the firmware from a file server, you load new firmware through FTP or TFTP from a file server. You can update the three firmware components—the management system firmware, the firmware web pages, and the radio firmware—individually or all at once. It is simplest to update all the components at once, but in some situations you might want to update them individually.

Full Update of the Firmware Components

To update all the firmware components at the same time, click **From File Server** on the Fully Update Firmware line on the Cisco Services Setup page. The Update All Firmware From File Server page appears. Figure 10-4 shows the Update All Firmware From File Server page.

Figure 10-4 Update All Firmware From File Server Page

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 00:21:18
Current Version of System Firmware:				10.13			
Current Version of Web Pages:				10.13			
Current Version of Radio Firmware:				4.10			
New File for All Firmware:				<input type="text"/>			
File Server Setup							
<input type="button" value="Update From Server"/>				<input type="button" value="Save To Server"/>	<input type="button" value="Done"/>	<input type="button" value="Cancel"/>	

Follow these steps to update all three firmware components from a file server:

- Step 1** Click the File Server Setup link to enter the FTP settings. The FTP Setup page appears. Figure 10-5 shows the FTP Setup page.

Figure 10-5 FTP Setup Page

Map Help Uptime: 02:37:33

File Transfer Protocol: FTP

Default File Server:

FTP Directory:

FTP User Name: anonymous

FTP User Password:

Apply OK Cancel Restore Defaults

- Step 2** Enter the FTP settings on the FTP Setup page.
- Select FTP or TFTP from the File Transfer Protocol pull-down menu. FTP (File Transfer Protocol) is the standard protocol that supports transfers of data between local and remote computers. TFTP (Trivial File Transfer Protocol) is a relatively slow, low-security protocol that requires no user name or password.
 - In the Default File Server entry field, enter the IP address of the server where the access point should look for FTP files.
 - In the FTP Directory entry field, enter the directory on the server where FTP files are located.
 - In the FTP User Name entry field, enter the user name assigned to the FTP server. If you selected TFTP, you can leave this field blank.
 - In the FTP Password entry field, enter the password associated with the user name. If you selected TFTP, you can leave this field blank.
 - Click **OK**. You return automatically to the Update All Firmware Through File Server page.
- Step 3** On the Update All Firmware Through File Server page, type the filename of the new firmware image file in the New File for All Firmware entry field.
- Step 4** Click **Browser Update Now** to load and install the new firmware. When the update is complete, the access point automatically reboots.

Selective Update of the Firmware Components

To update firmware components individually, click **From File Server** on the Selectively Update Firmware line on the Cisco Services Setup page. The Update Firmware From File Server page appears. Figure 10-6 shows the Update Firmware From File Server page.

Figure 10-6 Update Firmware From File Server Page

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 00:24:33
Current Version of <u>System Firmware</u> :			10.13				
Current Version of <u>Web Pages</u> :			10.13				
Current Version of <u>Radio Firmware</u> :			4.10				
New File for System Firmware:			<input type="text"/>				
New File for Web Pages:			<input type="text"/>				
New File for Radio Firmware:			<input type="text"/>				
<u>File Server Setup</u>							
			Update From Server		Save To Server		Done Cancel

To update one of the three firmware components from the file server, follow the steps listed in the “Full Update of the Firmware Components” section on page 10-5, but in Step 3, type the filenames of the firmware components you want to update in the components’ entry fields. Click **Browser Update Now** to load and install the new firmware. When the update is complete, the access point automatically reboots.

Retrieving Firmware and Web Page Files

You can retrieve and download the following files from an access point to your computer’s hard drive:

- System firmware
- Web pages
- Radio firmware

These files can be downloaded selectively or at one time, depending on which page you select from which to retrieve them. To retrieve all firmware and web page files, browse to the Update All Firmware Through Browser page and click **Retrieve All Firmware Files**. To selectively retrieve these files, browse to the Selectively Update Firmware Through Browser or From File Server and select the files you wish to retrieve.

Follow these steps to retrieve and download all files.

-
- Step 1** From the Services section of the eSetup page, click **Cisco Services**. The Cisco Services Setup page appears.
 - Step 2** On the Fully Update Firmware: line, click **Through Browser**. The Update All Firmware Through Browser page appears.
 - Step 3** Click **Retrieve All Firmware Files**. A file download window appears informing you that you are downloading the file from the IP address of your access point and prompting you to select a download method.
 - Step 4** Click **Save** to download the file to your computer. A Save As window appears.
 - Step 5** Navigate to the drive and folder on your computer where you want to save the file.
 - Step 6** Click **Save**. A File Download window appears and provides the progress of the download operation.
 - Step 7** Click **Close** when the download is complete.
-

Follow these steps to retrieve and download selected files.

-
- Step 1** From the Selectively Update Firmware line on the Cisco Services Setup page, click **Through Browser** or **From File Server**. The Cisco Services Setup page appears.
 - Step 2** Click on the link for the file you wish to retrieve. A file download window appears informing you that you are downloading the file from the IP address of your access point and prompting you to select a download method.
 - Step 3** Click **Save** to download the file to your computer. A Save As window appears.
 - Step 4** Navigate to the drive and folder on your computer where you want to save the file.
 - Step 5** Click **Save**. A File Download window appears and provides the progress of the download operation.

Step 6 Click **Close** when the download is complete.

Distributing Firmware

You use the Distribute Firmware page to distribute the access point's firmware to other Cisco Aironet access points. Figure 10-7 shows the Distribute Firmware page. The distributing access point and the access points that receive the firmware must have a Default Gateway setting other than the default setting, which is 255.255.255.255 (the Default Gateway setting is on the Express Setup and Routing Setup pages).

The access point sends its firmware to all the access points on your network that:

- Are running access point firmware version 10.00 or newer
- Can detect the IP multicast query issued by the distributing access point (network devices such as routers can block multicast messages)
- Have their web servers enabled for external browsing (see the “Entering Web Server Settings and Setting Up Access Point Help” section on page 7-7).
- Have the same HTTP port setting as the distributing access point (the HTTP port setting is on the Web Server Setup page)
- Have a Default Gateway setting other than the default setting, which is 255.255.255.255
- If they have User Manager enabled, contain in their User Lists a user with the same username, password, and capabilities as the user performing the distribution (the person logged in on the distributing access point)

Figure 10-7 *Distribute Firmware Page*

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 00:26:31
Current User:			admin				
Distribute All Firmware:			<input checked="" type="radio"/> yes <input type="radio"/> no				
Current Version of System Firmware:			10.13				<input checked="" type="checkbox"/>
Current Version of Web Pages:			10.13				<input checked="" type="checkbox"/>
Current Version of Radio Firmware:			4.10				<input checked="" type="checkbox"/>
							<input type="button" value="Start"/> <input type="button" value="Abort"/>

Follow this link path in the browser interface to reach the Distribute Firmware page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.
3. On the Cisco Services page, click **Distribute Firmware to other Cisco Devices**.

Follow these steps to distribute firmware to other access points:

-
- Step 1** Follow the link path to reach the Distribute Firmware page.
- Step 2** To distribute all three firmware components at once, verify that **yes** is selected for Distribute All Firmware. This is the default setup for the Distribute Firmware page.
- To distribute the firmware components individually, select **no** for Distribute All Firmware, and click the checkboxes for the components you want to distribute.
- Step 3** Click **Start**. The access point's firmware is distributed to the access points on your network. To cancel the distribution, click **Abort**.
- When the distribution is complete, the access points that received the firmware automatically reboot.
-

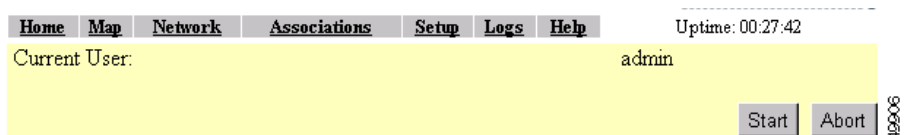
Distributing a Configuration

You use the Distribute Configuration page to distribute the access point's configuration to other Cisco Aironet access points. Figure 10-8 shows the Distribute Configuration page. The distributing access point and the access points that receive the configuration must have a Default Gateway setting other than the default setting, which is 255.255.255.255 (the Default Gateway setting is on the Express Setup and Routing Setup pages).

The access point sends its entire system configuration except for its IP identity information and its User List. The configuration is sent and applied to all the access points on your network that:

- Are running access point firmware version 10.05 or newer
- Can detect the IP multicast query issued by the distributing access point (network devices such as routers can block multicast messages)
- Have their web servers enabled for external browsing (see the “Entering Web Server Settings and Setting Up Access Point Help” section on page 7-7).
- Have the same HTTP port setting as the distributing access point (the HTTP port setting is on the Web Server Setup page)
- Have a Default Gateway setting other than the default setting, which is 255.255.255.255 (the Default Gateway setting is on the Express Setup and Routing Setup pages)
- If they have User Manager enabled, contain in their User Lists a user with the same user name, password, and capabilities as the user performing the distribution (the person logged in on the distributing access point)

Figure 10-8 Distribute Configuration Page



Follow this link path in the browser interface to reach the Distribute Configuration page:

1. On the Summary Status page, click **Setup**.

2. On the Setup page, click **Cisco Services Setup**.
3. On the Cisco Services page, click **Distribute Configuration to other Cisco Devices**.

Follow these steps to distribute the access point's configuration to other access points:

-
- Step 1** Follow the link path to reach the Distribute Configuration page.
- Step 2** Click **Start**. The access point's configuration, except for its IP identity and its User List, is distributed to the access points on your network. To cancel the distribution, click **Abort**.
-

Downloading, Uploading, and Resetting the Configuration

You use the System Configuration Setup page to download the current access point configuration to a local drive, upload a configuration from a local drive or file server, and reset the configuration to default settings. You can also use the System Configuration Setup page to restart the access point. Figure 10-9 shows the System Configuration Setup page.

Figure 10-9 System Configuration Setup Page

Home Map Network Associations **Setup** Logs Help Uptime: 00:28:45

"WARM" RESTART SYSTEM NOW "COLD" RESTART SYSTEM NOW

[Download Non-Default System Configuration Except IP Identity](#)

Reset System Factory Defaults Except IP Identity

[Download Non-Default System Configuration](#) [Download All System Configuration](#)

Reset All System Factory Defaults

Additional System Configuration File: Browse...

Read Config File from Server Browser Update Now Done

Follow this link path in the browser interface to reach the System Configuration Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.
3. On the Cisco Services page, click **Manage System Configuration**.

Downloading the Current Configuration

Follow these steps to download the access point's current configuration to your hard drive or to a mapped network drive:

- Step 1** Follow the link path to the System Configuration Setup page.
- Step 2** If your web browser is Microsoft Windows Internet Explorer, use the download configuration links to save the configuration file:
 - Click **Download System Configuration Except IP Identity** to save an .ini file containing the current configuration except for the access point's IP address.

- To save the current non-default configuration including the access point's IP address, click **Download Non-Default System Configuration**.
- To save the current default and non-default configuration including the access point's IP address, click **Download All System Configuration**.

If your web browser is Netscape Communicator, use your right mouse button to click the download configuration links and select **Save link as** in the pop-up menu. If you click the links with your left mouse button, Netscape Communicator displays the text file but does not open the Save as window.

- Step 3** When the Save as window appears, select the drive and directory where you want to save the file, and provide a filename for the configuration file. Click **Save**.
-

Uploading a Configuration

You can upload a configuration file to the access point from your hard drive or a mapped network drive, or you can upload a configuration from a file server.

Uploading from a Local Drive

Follow these steps to upload a configuration file from your hard drive or a mapped network drive:

-
- Step 1** Follow the link path in the browser interface to reach the System Configuration Setup page.
- Step 2** If you know the exact path and filename of the configuration file, type it in the Additional System Configuration File entry field.
- If you aren't sure of the exact path to the configuration file, click **Browse...** next to the entry field. When the File Upload window appears, go to the directory that contains the configuration file and select the file. Click **Open**.
- Step 3** When the filename appears in the Additional System Configuration File entry field, click **Browser Update Now**.

The configuration file is loaded and applied in the access point.

Uploading from a File Server

Follow these steps to upload a configuration file from a file server:

- Step 1** Before you load a configuration file from a server, you need to enter FTP settings for the server. If you have already entered the FTP settings, skip to Step 3.

Follow this link path in the browser interface to reach the FTP Setup page:

- a. On the Summary Status page, click **Setup**
- b. On the Setup page, click **FTP**

The FTP Setup page appears. Figure 10-10 shows the FTP Setup page.

Figure 10-10 FTP Setup Page

Map Help Uptime: 02:37:33

File Transfer Protocol: FTP

Default File Server:

FTP Directory:

FTP User Name: anonymous

FTP User Password: *****

Apply OK Cancel Restore Defaults 40018

- Step 2** Enter the FTP settings on the FTP Setup page.
- a. Select FTP or TFTP from the File Transfer Protocol pull-down menu. FTP (File Transfer Protocol) is the standard protocol that supports transfers of data between local and remote computers. TFTP (Trivial File Transfer Protocol) is a relatively slow, low-security protocol that requires no user name or password.
 - b. In the Default File Server entry field, enter the IP address of the server where the access point should look for FTP files.
 - c. In the FTP Directory entry field, enter the directory on the server where FTP files are located.
 - d. In the FTP User Name entry field, enter the user name assigned to the FTP server. If you selected TFTP, you can leave this field blank.

- e. In the FTP Password entry field, enter the password associated with the user name. If you selected TFTP, you can leave this field blank.
 - f. Click **OK**. You return automatically to the Setup page.
- Step 3** Follow the link path in the web browser to reach the System Configuration Setup page.
- Step 4** Click **Read Config File From Server**. The management system checks the server for several possible configuration filenames while attempting to load the configuration file. If the management system doesn't find the first filename, it continues to the next until it finds the file and loads it. It checks the server for the following names in the following order:
- a. [system name].ini
 - b. [IP address].ini
 - c. [boot file from DHCP/BOOTP server].ini
 - d. [boot file from DHCP/BOOTP server].ini by TFTP
-

Resetting the Configuration

You can reset the access point configuration to the default settings without resetting the access point's IP identity, or you can reset the configuration to the default settings including the IP identity. If you reset the access point's IP identity, however, you might lose your browser connection to the access point.

Two buttons on the System Configuration Setup page reset the configuration to defaults:

- **Reset System Factory Defaults Except IP Identity**—this button returns all access point settings to their factory defaults *except*:
 - The access point's IP address, subnet mask, default gateway, and boot protocol
 - The users in the User Manager list
 - The SNMP Administrator Community name
- **Reset All System Factory Defaults**—this button returns all access point settings to their factory defaults *except*:

- The users in the User Manager list
- The SNMP Administrator Community name

**Note**

To completely reset all access point settings to defaults, follow the steps in the “Resetting to the Default Configuration” section on page 13-43.

Follow these steps to reset the configuration to default settings:

- Step 1** Follow the link path to reach the System Configuration Setup page. Figure 10-9 shows the System Configuration Setup page. The link path is listed under Figure 5-9.
- Step 2** Click **Reset System Factory Defaults Except IP Identity** to reset the access point configuration to the default settings without resetting the access point’s IP identity. Click **Reset All System Factory Defaults** to reset the configuration to the default settings including the IP identity.

**Note**

If you reset the access point’s IP identity, you might lose your browser connection to the access point.

Restarting the Access Point

Use the System Configuration Setup page to restart the access point.

- Click **“Warm” Restart System Now** to perform a warm restart of the access point. A warm restart reboots the access point.
- Click **“Cold” Restart System Now** to perform a cold restart of the access point. A cold restart is the equivalent of removing and then reapplying power for the access point.



Management System Setup

This chapter explains how to set up your access point to use SNMP, Telnet, or the console port to manage the access point. This chapter contains the following sections:

- SNMP Setup, page 11-2
- Console and Telnet Setup, page 11-5
- Using Secure Shell, page 11-6

SNMP Setup

Use the SNMP Setup page to configure the access point to work with your network's SNMP station. Figure 11-1 shows the SNMP Setup page.

Figure 11-1 *SNMP Setup Page*

Map Help Uptime: 00:30:11

Simple Network Management Protocol (SNMP): ☒ Enabled ☐ Disabled

System Description: Cisco AP350 11.0

System Name: CiscoAP350

System Location:

System Contact:

SNMP Trap Destination:

SNMP Trap Community:

[Browse Management Information Base \(MIB\)](#)

Apply OK Cancel Restore Defaults

Follow this link path to reach the SNMP Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **SNMP** in the Services section of the page.

Settings on the SNMP Setup Page

The SNMP Setup page contains the following settings:

- Simple Network Management Protocol (SNMP)—Select **Enabled** to use SNMP with the access point.
- System Description—The system's device type and current version of firmware.

- **System Name**—The name of the access point. The name in this field is reported to your SNMP's management station as the name of the device when you use SNMP to communicate with the access point.
- **System Location**—Use this field to describe the physical location of the access point, such as the building or room in which it is installed.
- **System Contact**—Use this field to name the system administrator responsible for the access point.
- **SNMP Trap Destination**—The IP address of the SNMP management station. If your network uses DNS, enter a host name that resolves into an IP address.
- **SNMP Trap Community**—The SNMP community name required by the trap destination before it records traps sent by the access point.

The Browse Management Information Base (MIB) link at the bottom of the SNMP Setup page leads to the Database Query page.

Using the Database Query Page

Use the Database Query page to find and change the value of many access point managed objects. Figure 11-2 shows the Database Query page.

Figure 11-2 Database Query Page

Home Map Network Associations **Setup** Logs Help Uptime: 03:16:23

OID

Value

Get Set Reset 49006

Follow this link path to reach the Database Query page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **SNMP** in the Services section of the page.
3. On the SNMP Setup page, click **Browse Management Information Base (MIB)**.

Settings on the Database Query Page

The Database Query page contains the following entry fields and buttons:

- **OID**—Type the object identifier (OID) in the OID field. You can use the integer or ASCII version of the OID. If you use the integer version of the OID, you must type the entire OID string (1.3.7.2.13.78.5.6, for example). If you use the ASCII name, you can often use the object's name as specified in the appropriate MIB (*enableSNMP*, for example).
- **Value**—When you click **Get**, the object's value appears in the Value field. If you want to assign a value to an object, you type an SNMP value in this field and click **Set**.
- **Get**—Click **Get** to find an object's value.
- **Set**—Click **Set** to assign a value to an object.
- **Reset**—Click **Reset** to return the page to default settings.

Changing Settings with the Database Query Page

Follow these steps to change an access point setting from the Database Query page:

-
- Step 1** Type the object identifier (OID) in the OID field. You can use the integer or ASCII version of the OID. If you use the integer version of the OID, you must type the entire OID string (*1.3.7.2.13.78.5.6*, for example). If you use the ASCII name, you can often use the object's name as specified in the appropriate MIB (*enableSNMP*, for example). MIBs supported by the access point are listed in the “Supported MIBs” section on page 2-25.
- Step 2** Click **Get**. The current value for the setting appears in the Value field.
- Step 3** Modify the value in the Value field.
- Step 4** Click **Set**. The new value is set on the access point.



Note If the object is read-only, the value is not changed when you click **Set**.

Console and Telnet Setup

Use the Console/Telnet Setup page to configure the access point to work with a terminal emulator or through Telnet. Figure 11-3 shows the Console/Telnet Setup page.

Figure 11-3 Console/Telnet Setup Page

The screenshot shows the 'Console/Telnet Setup' page with a yellow background. At the top left are 'Map' and 'Help' buttons. At the top right is the 'Uptime: 03:17:44' text. The main area contains the following settings:

- Baud Rate: 9600 (dropdown)
- Parity: None (dropdown)
- Data Bits: 8 (dropdown)
- Stop Bits: 1 (dropdown)
- Flow Control: SW Xon/Xoff (dropdown)
- Terminal Type: teletype (dropdown)
- Columns (64-132): 80 (text input)
- Lines (16-50): 25 (text input)
- Telnet: ☒ Enabled ☐ Disabled

At the bottom right are four buttons: 'Apply', 'OK', 'Cancel', and 'Restore Defaults'. A vertical label '49204' is on the far right edge.

Follow this link path to reach the Console/Telnet Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Console/Telnet** in the Services section of the page.

Settings on the Console/Telnet Page

The Console/Telnet Setup page contains the following settings:

- **Baud Rate**—The rate of data transmission expressed in bits per second. Select a baud rate from 110 to 115,200, depending on the capability of the computer you use to open the access point management system.
- **Parity**—An error-detecting process based on the addition of a parity bit to make the total number of bits Odd or Even. The default setting, None, uses no parity bit.

- Data Bits—The default setting is 8.
- Stop Bits—The default setting is 1.
- Flow Control—Defines the way that information is sent between pieces of equipment to prevent loss of data when too much information arrives at the same time on one device. The default setting is SW Xon/Xoff.
- Terminal Type—The preferred setting is ANSI, which offers graphic features such as reverse video buttons and underlined links. Not all terminal emulators support ANSI, so the default setting is Teletype.
- Columns—Defines the width of the terminal emulator display within the range of 64 characters to 132 characters. Adjust the value to get the optimum display for your terminal emulator.
- Lines—Defines the height of the terminal emulator display within the range of 16 characters to 50 characters. Adjust the value to get the optimum display for your terminal emulator.
- Enable Telnet—The default setting is Yes. Select **No** to prevent Telnet access to the management system.

Using Secure Shell

Secure Shell (SSH) is a program that provides a cryptographically secure replacement for Telnet that is considered the de facto protocol for remote logins. SSH runs in the Application Layer of the TCP/IP stack. SSH provides a secure connection over the Internet providing strong user authentication. SSH protects the privacy of transmitted data (such as passwords, binary data, and administrative commands) by encrypting it.

SSH clients make SSH relatively easy to use and are available on most computers including those that run Windows or a type of UNIX. SSH clients are also available on some handheld devices.

SSH on the access point is enabled by default. When user manager is enabled, SSH uses the same usernames and passwords established by the user manager.

Newer computers have the SSH client installed. If your computer does not have the SSH client installed, you must procure and install it before you can proceed. You can download the latest SSH client from the following site:

<http://ssh.com/>

After you have downloaded and installed the client on your computer, launch your SSH client and make the connection to the access point through it.



Special Configurations

This chapter describes how to set up the access point in network roles other than as a root unit on a wired LAN. You can set up an access point as a repeater to extend the range of a wireless network, and you can use Hot Standby mode to use an access point as a backup unit in areas where you need extra reliability. Both configurations require two access points that support and rely upon each other.

This chapter contains the following sections:

- Setting Up a Repeater Access Point, page 12-2
- Using Hot Standby Mode, page 12-6

Setting Up a Repeater Access Point

A repeater access point is not connected to the wired LAN; it is placed within radio range of an access point connected to the wired LAN to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication.

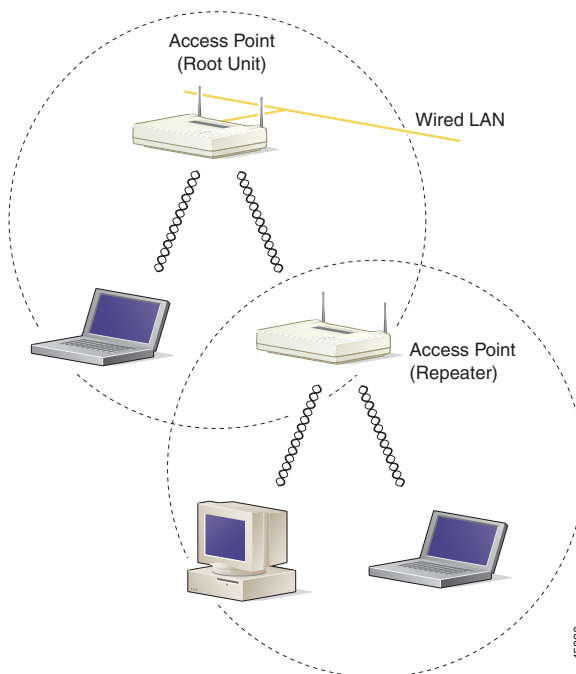
The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the greatest performance for the client. When you configure an access point as a repeater, the access point's Ethernet port does not forward traffic. Figure 12-1 shows an access point acting as a repeater.



Note

Non-Cisco client devices might have difficulty communicating with repeater access points.

Figure 12-1 Access Point as Repeater



You can set up a chain of several repeater access points, but throughput for client devices at the end of the repeater chain will be quite low. Because each repeater must receive and then re-transmit each packet on the same channel, throughput is cut in half for each repeater you add to the chain.

Omni-directional antennas, like the ones that ship with your access point, are best suited for repeater access points.

If you use EAP authentication on your wireless network, you can set up the repeater access point to authenticate using LEAP. See the “Setting up a Repeater Access Point as a LEAP Client” section on page 8-27 for instructions on enabling LEAP on a repeater.

Follow these steps to set up a repeater access point:

-
- Step 1** Use the *Quick Start Guide: Cisco Aironet Access Points* and the information in this manual to set up an access point as a root unit on the wired LAN.
- Step 2** Write down the root-unit access point’s MAC address. The MAC address appears on the label on the bottom of the access point.
- Step 3** The repeater access point will need to duplicate some of the root access point’s settings. If the root access point has been completely configured, browse to the root access point and write down the following settings so you can refer to them when you set up the repeater access point:

- SSID (found on the Express Setup page)
- Default IP Subnet Mask (also on the Express Setup page)

**Note**

You can also rely on the DHCP server to assign a default IP subnet mask.

- Default Gateway (also on the Express Setup page)

**Note**

You can also rely on the DHCP server to assign a default gateway.

- Data rates (found on the AP Radio Hardware page)
- WEP settings (found on the AP Radio Data Encryption page)
- Authentication Types (found on the AP Radio Data Encryption page)

If the root access point settings have not been changed from the factory defaults, you don't need to write them down. If you reconfigure the root access point, however, you must enter the same settings on the repeater access point.

- Step 4** Place the repeater access point within radio range of the root access point.
- Step 5** For a 340 series access point, plug one end of the power cord into the access point's power connector. Plug the other end into an electrical outlet.
- Step 6** For a 350 series access point, plug an Ethernet cable into the access point's Ethernet port. Plug the other end of the Ethernet cable into the side of the power injector labelled *To AP*.



Note The repeater access point will not be connected to the wired LAN, so do not run Ethernet cable from the power injector to a switch.

- Step 7** Plug the power injector's power cable into an electrical outlet.



Note Step 8, Step 9, and Step 10 describe opening the access point management system using a terminal emulator, but you can use a crossover cable instead. Use a crossover cable to connect the access point's Ethernet port to the Ethernet connection on a computer and browse to the access point's IP address. If you use a crossover cable to open the management system, skip to Step 11.

- Step 8** Attach a nine-pin, male-to-female, straight-through serial cable to the access point's serial port. Plug the other end of the serial cable into the COM 1 or COM 2 port on a computer.
- Step 9** Use a terminal emulator to open the access point's management system. Assign these port settings to the terminal emulator: 9600 baud, 8 data bits, No parity, 1 stop bit, and Xon/Xoff flow control.
- Step 10** When the terminal emulator connects with the access point, press = to display the access point's Summary Status page. If the repeater access point has never been configured before, the Express Setup page will appear instead of the Summary Status page.
- Step 11** On the Express Setup page, enter the same SSID that is set on the root access point.

**Note**

Step 12 and Step 13 describe assigning a static IP address, subnet mask, and gateway to the repeater. However, you can rely on your DHCP server to assign these settings if you do not need them to remain fixed. If the repeater will use the DHCP server, skip to Step 14.

- Step 12** On the Express Setup page, enter a fixed IP address for the repeater access point in the Default IP address field.
- Step 13** Also on the Express Setup page, enter the same settings in the Default IP Subnet Mask and Default Gateway fields that are on the root access point.
- Step 14** On the Boot Server Setup page, select **none** for the Configuration Server Protocol. This setting will maintain a fixed IP address for the repeater access point.
- If the root access point configuration has not been changed from the factory defaults, skip to Step 18.
- Step 15** On the AP Radio Hardware page, enter the same settings for Data Rates that are on the root access point.
- Step 16** On the AP Radio Data Encryption page, enter the same WEP key settings that are on the root access point.
- Step 17** Also on the AP Radio Data Encryption page, select the same Authentication Types that are on the root access point.
- Step 18** On the AP Radio Advanced page, enter the root access point's MAC address in the Specified access point 1 entry field.
- Step 19** On the Express Setup page, select **Repeater Access Point** as the Role in Radio Network. The access point reboots when you apply this setting.
- Step 20** The status LED on the root access point should be steady green, indicating that at least one client device is associated with it. The status LED on the repeater access point is steady green when it is associated with the root access point and has client devices associated with it. The repeater's status LED is steady for 7/8 of a second and off for 1/8 of a second when it is associated with the root access point but has no client devices associated with it. The repeater access point should also appear as associated with the root access point in the root access point's Association Table.

Using Hot Standby Mode

Hot Standby mode designates an access point as a backup for another access point. The standby access point is placed near the access point it monitors, configured exactly the same as the monitored access point. The standby access point associates with the monitored access point as a client and queries the monitored access point regularly through both the Ethernet and the radio. If the monitored access point fails to respond, the standby access point comes online and takes the monitored access point's place in the network.

Except for the IP address, the standby access point's settings should be identical to the settings on the monitored access point. You use the Hot Standby page to set up the standby access point. Figure 12-2 shows the Hot Standby page.

Figure 12-2 Hot Standby Page

Map

Help

Uptime: 00:36:15

Service Set ID (SSID)

TestAP 2

MAC Address For the Monitored AP:

00:00:00:00:00:00

Polling Frequency:

1

(Seconds)

Polling Tolerance Duration:

5

(Seconds)

Current State:

Hot Standby is not running.

Current Status:

Hot Standby unit is OK.

Start Hot Standby Mode

STOP Hot Standby Mode

Apply

OK

Cancel

Restore Defaults

Follow this link path to reach the Hot Standby page:

- On the Summary Status page, click **Setup**.
- On the Setup page, click **Cisco Services** under Services.
- On the Cisco Services Setup page, click **Hot Standby Management**.



Note

Wireless client devices associated to the standby access point lose their connections during the hot standby setup process.

Follow these steps to enable Hot Standby mode:

-
- Step 1** On the standby access point, duplicate the settings that are entered on the monitored access point. Critical settings include:
- SSID (found on the Express Setup page)
 - Default IP Subnet Mask (also on the Express Setup page)
 - Default Gateway (also on the Express Setup page)
 - Data rates (found on the AP Radio Hardware page)
 - WEP settings (found on the AP Radio Data Encryption page)
 - Authentication Types (found on the AP Radio Data Encryption page)
- Step 2** On the standby access point, browse to the AP Radio Identification page:
- a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **Identification** in the AP Radio row under Network Ports.
- Step 3** Select **no** for the Adopt Primary Port Identity option and click **Apply**. The access point reboots.
- After the access point reboots, the radio has its own identity: the radio IP and MAC addresses are different from the Ethernet addresses. The default IP address for the radio is 10.0.0.2.
- In two situations, you might need to change the radio IP address from its default setting:
- You must change the radio IP address if you need to use 10.0.0.2 for the Ethernet IP address. The Ethernet and radio ports on the standby access point must have different IP addresses.
 - You must change the radio IP address if you need to browse to the standby access point through its radio port. If you need to browse to the access point through the radio port, assign the port an IP address on the same subnet as the Ethernet IP address.
- Step 4** After the access point reboots, browse to the Hot Standby page.
- Step 5** Enter the monitored access point's SSID in the Service Set ID entry field.
- Step 6** Enter the monitored access point's MAC address in the MAC Address For the Monitored AP entry field.

- Step 7** Enter the number of seconds between each query the standby access point sends to the monitored access point.
- Step 8** Enter the number of seconds the standby access point should wait for a response from the monitored access point before it assumes that the monitored access point has malfunctioned.
- Step 9** Click **Start Hot Standby Mode**. The standby access point becomes a client device associated to the monitored access point.
- Step 10** Click the browser's refresh button to verify that the Current State line on the Hot Standby Setup page states that Hot Standby is initialized.

**Note**

If the monitored access point malfunctions and the standby access point takes its place, repeat the hot standby setup on the standby access point when you repair or replace the monitored access point. The standby access point does not revert to standby mode automatically.

**Note**

If you need to browse to the standby access point from a workstation that is on a different subnet than the standby access point, set the IP address on the standby radio interface to a subnet that is compatible with the workstation's IP address. Use the AP Radio ID page to enter a new IP address for the standby radio.



Diagnostics and Troubleshooting

This chapter describes the diagnostic pages in the management system and provides troubleshooting procedures for basic problems with the access point. For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at <http://www.cisco.com/tac>. Select **Wireless LAN** under Top Issues.

Sections in this chapter include:

- Using Diagnostic Pages, page 13-2
- Using Command-Line Diagnostics, page 13-19
- Tracing Packets, page 13-32
- Checking the Top Panel Indicators, page 13-37
- Checking Basic Settings, page 13-40
- Resetting to the Default Configuration, page 13-43

Using Diagnostic Pages

The management system contains three diagnostic pages that provide detailed statistics and event records for the access point:

- The Network Diagnostics Page provides access to radio diagnostic tests and provides links to the VLAN Summary Status and SSID statistics pages for accesspoint radios.
- The Network Ports Page lists statistics on data transmitted and received by the access point.
- The Event Log Page lists network events.

Each page is described in the sections below.

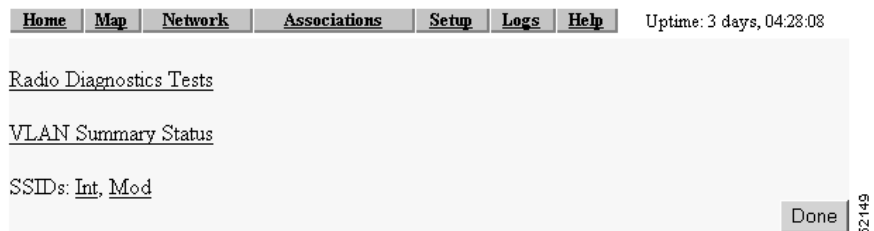
Network Diagnostics Page

Use the Network Diagnostics page to access the following diagnostic pages:

- Radio diagnostics tests
- VLAN Summary Status page
- SSID pages for the internal or module radio

Figure 13-1 shows the Network Diagnostics page.

Figure 13-1 Network Diagnostics Page



Follow this link path to reach the Network Diagnostics page:

1. On the Summary Status page or Setup page, click **Diagnostics** in the Network Ports row.

Selections on the Network Diagnostics Page

The Network Diagnostics page contains the following selections:

- Radio Diagnostics Tests
- VLAN Summary Status
- SSIDs: Int, Mod

Radio Diagnostics Tests

Click **Radio Diagnostics Tests** to access the Radio Diagnostics page and conduct a carrier test (Figure 13-2).

Figure 13-2 *Radio Diagnostics Page*



The carrier test helps you determine which radio frequencies contain the most radio activity and noise that could interfere with radio signals to and from the access point.

Use the carrier test to determine the best frequency for the access point to use. When you conduct a carrier test, make sure all wireless networking devices within range of the access point are operating to make the test results reflect a realistic radio environment.

When you click **Start**, the radio scans the access point's available frequencies and displays the radio activity in the Carrier Test window.



Note

The access point drops all associations with wireless networking devices during the carrier test.

Carrier Test

The carrier test measures the amount of radio activity on each frequency available to the access point. Use the carrier test to determine the best frequency for the access point to use. When you conduct a carrier test, make sure all wireless networking devices within range of the access point are operating to make the test results reflect a realistic radio environment.

When you click **Start Carrier Test**, the radio scans the access point's available frequencies and displays the radio activity in the Carrier Test window.

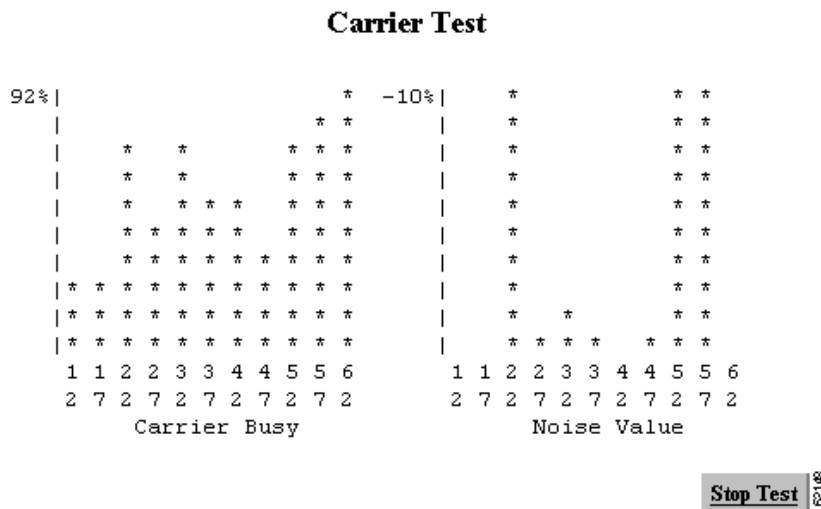


Note

The access point drops all associations with wireless networking devices during the carrier test.

Figure 13-3 shows an example Carrier Test window.

Figure 13-3 Carrier Test Window



The bar graph on the left side of the window displays the percentage used for each frequency; the highest current percentage used is labeled on the top left of the graph. In this example, the highest percentage used for any frequency is 92. The

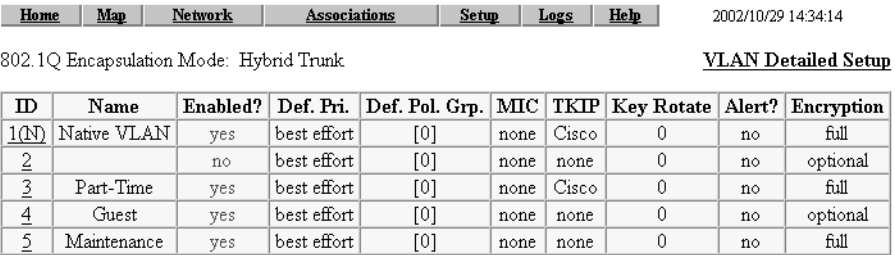
access point's available frequencies are listed vertically across the bottom of the graph, from 2412 to 2462 GHz. The access point's channel 1 is 2412 GHz, channel 2 is 2417 GHz, and so on up to channel 11, which is 2462 GHz.

The bar graph on the right side of the window displays the amount of noise on each frequency. Noise is a measurement of the signal the radio receives when it is not receiving packets. Even in an environment in which the radio receives a great deal of noise, it might also receive a strong data signal. Click **Stop Test** in the window or on the Radio Diagnostics page to stop the test.

VLAN Summary Status

Click **VLAN Summary Status** to reach the VLAN Summary Status page for your access point. Figure 13-4 shows a typical VLAN Summary Status page.

Figure 13-4 VLAN Summary Status Page

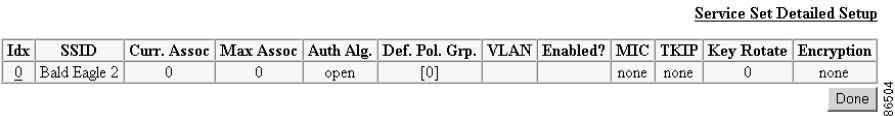


Clicking the **VLAN Detailed Setup** link at the top of the page takes you to the VLAN Setup page, from which you can add, remove, or edit your VLAN configuration.

Service Sets

The Service Sets link takes you to the AP Radio Service Set Summary Status page for your access point. shows a typical SSID Summary Status page for the radio.

Figure 13-5 AP Radio Module Service Set Summary Status Page



Clicking the **Service Set Detailed Setup** link at the top of the page takes you to the AP Radio Service Sets page, from which you can create, remove, or edit your SSID configuration.

Network Ports Page

The Network Ports page contains a table listing information for the access point's Ethernet and radio ports. Figure 13-6 shows a Network Ports page example.

Figure 13-6 Network Ports Page

Network Diagnostics

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 4 days, 23:27:31
Name		Ethernet ⁺	Root Radio	Bridge:BR350 West			
Status		Up	Up	Up			
Max. Mb/s		100.0	11.0	11.0			
IP Addr.		10.84.137.71	10.84.137.71	10.84.137.71			
MAC Addr.		00409631535e	00409631535e	00409631535e			
Radio SSID			bridge				
Receive							
unicast pkts.		33477	1043	114			
multicast pkts.		948580	0	589			
total bytes		48992558	156555	131190			
errors		0	0	0			
discards		0	0	0			
forwardable pkts.		132981	39171	130			
filtered pkts.		0	1303	0			
Transmit							
unicast pkts.		45653	1073	117			
multicast pkts.		438983	213	773			
total bytes		37949231	288969	93564			
errors		0	18	0			
discards		0	0	0			
forwarded pkts.		524980	51601	240			

Click the **Network** link at the top of any main management system page to reach the Network Ports page, or click **Network Ports** on the Summary Status home page.

The Network Diagnostics link at the top of the Network Ports page leads to the Cisco Network Diagnostics page, where you can select diagnostic tests.

The Network Ports table is divided into three sections: identifying information and status, data received, and data transmitted. Each row in the table is described below.

Identifying Information and Status

- **Name**—Displays the name of the network interface port. An asterisk (*) next to the name identifies the port as the primary port for the access point.

The port names are links to a detailed page for each port. See the “Ethernet Port Page” section on page 13-9 for information on the Ethernet Port page and the “AP Radio Page” section on page 13-12 for information on the AP Radio Port page.

- **Status**—Displays one of three possible operating states for the port:
 - **Up**—The port is operating properly.
 - **Down**—The port is not operating.
 - **Error**—The port is operating but is in an error condition.
- **Max. Mb/s**—The maximum rate of data transmission in megabits per second.
- **IP Addr.**—The IP address for the port. When the access point is set up in standby mode the Ethernet and radio ports use different IP addresses. Use the AP Radio Identification page to assign an IP address to the radio port that is different from the Ethernet IP address. See the “Settings on the AP Radio Identification Page” section on page 3-9 for details on the AP Radio Identification page.
- **MAC (Media Access Control) Addr.**—The Media Access Control (MAC) address is a unique identifier assigned to the network interface by the manufacturer.
- **Radio SSID**—A unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity.

Data Received

- **Unicast pkts.**—The number of packets received in point-to-point communication.

- Multicast pkts.—The number of packets received that were sent as a transmission to a set of nodes.
- Total bytes—The total number of bytes received.
- Errors—The number of packets determined to be in error.
- Discards—The number of packets discarded by the access point due to errors or network congestion.
- Forwardable pkts.—The number of packets received by the port that was acceptable or passable through the filters.
- Filtered pkts.—The number of packets that were stopped or screened by the filters set up on the port.

Data Transmitted

- Unicast pkts.—The number of packets transmitted in point-to-point communication.
- Multicast pkts.—The number of packets transmitted that were sent as a transmission to a set of nodes.
- Total bytes—Total number of bytes transmitted from the port.
- Errors—The number of packets determined to be in error.
- Discards—The number of packets discarded by the access point due to errors or network congestion.
- Forwarded pkts.—The number of packets transmitted by the port that was acceptable or passable through the filters.

Ethernet Port Page

When you click **Ethernet** in the Network Ports table, the browser displays the Ethernet Port page. This page lists detailed statistics on the access point's Ethernet port. Figure 13-7 shows an Ethernet Port page example.

Figure 13-7 Ethernet Port Page

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 03:22:51	
Configuration					Set Properties			
Status of "fec0"	Up (primary)		Maximum Rate (Mb/s)		10.0			
IP Address	172.16.24.0		MAC Address		00409625854d			
Duplex	Full							
Statistics								
Receive			Transmit					
Unicast Packets	4620		Unicast Packets		3910			
Multicast Packets	98350		Multicast Packets		1193			
Total Bytes	13987582		Total Bytes		1238105			
Total Errors	0		Total Errors		0			
Discarded Packets	0		Discarded Packets		0			
Forwardable Packets	105199		Forwarded Packets		3379			
Filtered Packets	0							
Packet CRC Errors	0		Max Retry Packets		0			
Carrier Sense Lost	0		Total Collisions		0			
Late Collisions	0		Late Collisions		0			
Overrun Packets	0		Underrun Packets		0			
Packets Too Long	0							
Packets Too Short	0							
Packets Truncated	0							

40/11

Like the Network Ports page, the Ethernet Port page lists statistics in a table divided into sections. Each row in the table is explained in the following sections.

Configuration Information

- The top row of the Configuration section of the table contains a Set Properties link that leads to the Ethernet Hardware page.
- Status of “fec0”— “Fast Ethernet Controller” is part of Motorola's naming convention for the Ethernet device used by the access point. This field displays one of the three possible operating states for the port. The added term “primary” identifies the port as the primary port for the access point. Operating states include:
 - Up—The port is operating properly.
 - Down—The port is not operating.
 - Error—The port is in an error condition.
- Maximum Rate (Mb/s)—Maximum rate of data transmission in megabits per second.
- IP Address—The IP address of the port.
- MAC Address—The unique identifier assigned to the access point by the manufacturer.
- Duplex—The port's duplex setting, either half or full.

Receive Statistics

- Unicast Packets—The number of packets received in point-to-point communication.
- Multicast Packets—The number of packets received that were sent as a transmission to a set of nodes.
- Total Bytes—Total number of bytes received.
- Total Errors—Total number of packets determined to be in error.
- Discarded Packets—Packets discarded due to errors or network congestion.
- Forwardable Packets—Packets received by the port that were acceptable or passable through the filters.
- Filtered Packets—Packets that were stopped or screened by the filters set up on the port.
- Packet CRC Errors—Cyclic redundancy check (CRC) errors that were detected in a received packet.

- Carrier Sense Lost—The number of disconnects from the Ethernet network. Carrier sense lost events are usually caused by disconnected wiring.
- Late Collisions—Packet errors that probably were caused by over-long wiring problems. Late collisions could also indicate a failing NIC card.
- Overrun Packets—Ethernet packets that were discarded because the access point had a temporary overload of packets to handle.
- Packets Too Long—Ethernet packets that were larger than the maximum packet size of 1518 bytes.
- Packets Too Short—Ethernet packets that were shorter than the minimum packet size of 64 bytes.
- Packets Truncated—Corrupt or incomplete packets.

Transmit Statistics

- Unicast Packets—The number of packets transmitted in point-to-point communication.
- Multicast Packets—The number of packets transmitted that were sent as a transmission to a set of nodes.
- Total Bytes—Total number of bytes transmitted from the port.
- Total Errors—The number of packets determined to be in error.
- Discarded Packets—The number of packets discarded by the access point due to errors or network congestion.
- Forwarded Packets—The number of packets transmitted by the port that were acceptable or passable through the filters.
- Max Retry Packets—Packets which failed after being retried several times.
- Total Collisions—The number of packet collisions that occurred through this port.
- Late Collisions—Packet errors that were likely caused by overlong wiring problems. Could also indicate a failing NIC card.
- Underrun Packets—Packets failed to be sent because the access point was unable to keep up with the Ethernet controller.

AP Radio Page

When you click **AP Radio** in the Network Ports table, the browser displays the AP Radio Port page. This page lists detailed statistics on the access point's radio. Figure 13-8 shows an AP Radio Port page example.

Figure 13-8 AP Radio Port Page

[Home](#)
[Map](#)
[Network](#)
[Associations](#)
[Setup](#)
[Logs](#)
[Help](#)

Uptime: 3 days, 16:21:20

Options:
Detailed Config.
Detailed Stats.
Individual Rates

Apply

Configuration

Set Properties

Status of "awc0"	Up	Maximum Rate (Mb/s)	11.0
IP Address	10.0.0.1	MAC Address	00059a38421d
SSID	Test AP 2		
Operational Rates (Mb/s)	1.0B, 2.0B, 5.5B, 11.0B	Transmit Power (mW)	100

Statistics

Refresh

Receive		Alert	Transmit		Alert
Unicast Packets	33300	<input type="checkbox"/>	Unicast Packets	15555	<input type="checkbox"/>
Multicast Packets	0		Multicast Packets	31351	
Total Bytes	3431551		Total Bytes	16870368	
Total Errors	1		Total Errors	2	
Discarded Packets	1		Discarded Packets	0	
Forwardable Packets	25088		by CoS (0-7): 0, 0, 0, 0, 0, 0, 0, 0		
Filtered Packets	0		Forwarded Packets	70582	
Packet CRC Errors	51119453		Max Retry Packets	2	
Packet WEP Errors	0		Total Retries	4541	
Overrun Packets	0		Cancelled Assoc. Lost	0	
Duplicate Packets	1236		Cancelled AID	10	
Lifetime Exceeded	0		Lifetime Exceeded	0	
MIC Packets	0		MIC Packets	0	
MIC Errors	0		MIC Errors	0	
MIC Sequ. Errors	0				
MIC Auth. Errors	0				

Like the Network Ports and Ethernet Port pages, the AP Radio Port page lists statistics in a table divided into sections. Each row in the table is explained below.

Configuration Information

- The top row of the Configuration section of the table contains a Set Properties link that leads to the AP Radio Hardware page. See the “Entering Radio Hardware Information” section on page 3-11 for details on the AP Radio Hardware page.
- Status of “awc0”—*awc0* (Aironet Wireless Communications) is part of Cisco Aironet's naming convention for this radio. This field displays one of three possible operating states:
 - Up—The port is operating properly.
 - Down—The port is not operating.
 - Error—The port is in an error condition.
- Maximum Rate (Mbps)—Maximum rate of data transmission in megabits per second. Data rates set to basic are followed by B.
- IP Addr.—The IP address of the radio port.
- MAC (Media Access Control) Addr.—A unique identifier assigned to the network interface by the manufacturer.
- SSID—The unique identifier that client devices use to associate with the access point radio. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity.
- Operational Rates—The data transmission rates supported and enabled by the access point for communication with client devices.
- Transmit Power (mW)—The power level of radio transmission. You can reduce the transmit power to conserve power or reduce interference. Click **Set Properties** to display the AP Radio Hardware page, where you can change this setting.

Receive Statistics

- Unicast Packets—The number of packets received in point-to-point communication.
- Multicast Packets—The number of packets received that were sent as a transmission to a set of nodes.
- Total Bytes—The total number of bytes received.
- Total Errors—The total number of packets determined to be in error.

- Discarded Packets—Packets discarded due to errors or network congestion.
- Forwardable Packets—Packets received by the port that were acceptable or passable through the filters.
- Filtered Packets—Packets that were stopped or screened by the filters set up on the port.
- Packet CRC Errors—Cyclic redundancy check (CRC) errors that were detected in a received packet.
- Packet WEP Errors—Encryption errors received through this port.
- Overrun Packets—Packets that were discarded because the access point had a temporary overload of packets to handle.
- Duplicate Packets—Packets that were received twice because an acknowledgment was lost and the sender retransmitted the packet.
- Lifetime Exceeded—Fragmented packets that were dropped because it took too long to get the next fragment.

Transmit Statistics

- Unicast Packets—The number of packets transmitted in point-to-point communication.
- Multicast Packets—The number of packets transmitted that were sent as a transmission to a set of nodes.
- Total Bytes—The number of bytes transmitted from the port.
- Total Errors—The number of packets determined to be in error.
- Discarded Packets—The number of packets discarded by the access point due to errors or network congestion.
- Forwarded Packets—The number of packets transmitted by the port that were acceptable or passable through the filters.
- Max Retry Packets—The number of times request to send (RTS) reached the maximum retry number. Click **Set Properties** to display the AP Radio Hardware page, where you can set the maximum RTS value.
- Total Retries—The total number of retries that occurred through the radio port.
- Canceled Assoc. Lost—Packets dropped because a client device lost association with the access point.

- Canceled AID—Packets dropped by a repeater because it roamed to a different parent during a retransmission attempt.
- Lifetime Exceeded—Fragmented packets that were dropped because it took too long to deliver a fragment.
- MIC Packets—Total number of packets for which the access point has requested MIC has been requested to be calculated with the MMH algorithm before being submitted for transmission over this radio since system startup.
- MIC Errors—Total number of packets which have failed MIC calculation with the MMH algorithm before being submitted for transmission over this radio since system startup.
- MIC Sequ. Errors—Packet appear to have arrived either very late or out of sequence. This could be caused by a poor radio link or a replay.
- MIC Auth. Errors—The MIC signature is bad due to a calculation with the wrong cryptographic key. These errors could be caused by a simple misconfiguration of a WEP key, or it could be an attack

Display Options

Figure 13-8 shows the basic AP Radio Port page. Three display options provide more details on the port configuration and operating statistics. The basic page provides all the information needed to monitor and administer the port in normal operation. You might need the other display options in comprehensive site surveys or advanced system troubleshooting. To select a display option, click an option checkbox and click **Apply**.

The display options include:

- Detailed Config.—Details on the radio port configuration, including request to send (RTS) and data retry settings, firmware and bootblock version levels, and regulatory domain code.
- Detailed Stats.—Twenty additional statistical fields covering packet fragments, collisions, and other errors.
- Individual Rates—Data transmission statistics for each data rate (1, 2, 5, and 11 Mbps).

Event Log Page

The Event Log page lists access point events and provides links to the Event Display Setup and Event Log Summary pages. You can also open Station pages for devices listed in the event log. Figure 13-9 shows an Event Log page example.

Figure 13-9 Event Log Page

The screenshot shows the Event Log page interface. At the top, there are navigation tabs: Home, Map, Network, Associations, Setup, Logs, and Help. The 'Logs' tab is selected. To the right of the tabs, the uptime is displayed as 'Uptime: 03:26:14'. Below the tabs, there are two input fields: 'Index' with the value '0' and 'Number of Events' with the value '20'. To the right of these fields is a link 'Download Event Log'. Below the input fields, there is a section titled 'Press to Change Settings:' with four buttons: 'Next', 'Prev', 'Apply New', and 'Purge Log'. The main content area is titled 'Event Log' and has a link 'additional display filters' to its right. Below this title is a table with three columns: 'Time', 'Severity', and 'Description'. The table contains four rows of event data.

Time	Severity	Description
03:26:08	Info	Station Joe Smith Associated
03:26:08	Info	Station Joe Smith Authenticated
03:25:23	Info	Station 209.165.201.7 Reassociated
03:25:21	Info	Disassociating 209.165.201.7 , reason "Sender is Leaving (has left) BSS"

Click the **Logs** link at the top of any main management system page to reach the Event Log page.

Display Settings

Use the entry fields and the buttons at the top of the page to control the event list. Fields and buttons include:

- **Index**—Specifies the first event to display in the event list. The most recent event is 0; earlier events are numbered sequentially. To apply your entry, click **Apply New**.
- **Number of Events**—Specifies the number of events displayed on the page. To apply your entry, click **Apply New**.
- **Next**—Displays earlier events in the log.
- **Prev**—Displays more recent events in the log.
- **Apply New**—Changes the display by applying the settings in the Index and Number of Events fields.
- **Purge Log**—Permanently deletes all events from the log.

- **Additional Display Filters**—A link to the Event Display Setup page, where you can change time and severity level settings.

Log Headings

The event log is divided into three columns:

- **Time**—The time the event occurred. The log records time as cumulative days, hours, and minutes since the access point was turned on, or as wall-clock time if a time server is specified or if the time has been manually set on the access point.
- **Severity**—Events are classified as one of four severity levels depending on the event's impact on network operations. Severity levels include:
 - **Info (green)**—Indicates routine information; no error.
 - **Warning (blue)**—Indicates a potential error condition.
 - **Alert (magenta)**—Indicates that an event occurred which was pre-selected as something to be recorded in the log. A typical example of an alert would be a packet error condition. The Station page provides check boxes that activate reporting of packet errors to and from the station as alerts in the event log.
 - **FATAL (red)**—An event which prevents operation of the port or device. For operation to resume, the port or device usually must be reset.

Click the **Severity** heading to go to the Event Log Summary page, which lists total events for each severity level.

- **Description**—This column describes the nature or source of the event. If a network device is involved in the event, the device's MAC or IP address appears and provides a direct link to the device's Station page.

Saving the Log

To save the event log, click **Download Event Log**. In Microsoft Explorer, the log is saved as a text file. In Netscape Communicator, the log file is displayed on the screen, and you select **Save As** from Communicator's File pull-down menu to save the log.

Event Log Summary Page

The Event Log Summary page lists the total number of events that occurred at each severity level. Figure 13-10 shows an Event Log Summary page example.

Figure 13-10 Event Log Summary Page

<div> Home Map Network Associations Setup Logs Help </div>							Uptime: 03:27:11
Event Severity Level							Total Events
System Fatal							0
Protocol Fatal							0
Network Port Fatal							0
System Alert							0
Protocol Alert							0
Network Port Alert							0
External Alert							0
System Warning							0
Protocol Warning							2
Network Port Warning							0
External Warning							0
System Information							0
Protocol Information							21
Network Port Information							21
External Information							1

499415

Click the **Severity** heading on the Event Log page to reach the Event Log Summary page.

Using Command-Line Diagnostics

You can view diagnostic information about your access point with diagnostic commands. Enter the commands in the command-line interface (CLI) to display the information. You can open the CLI with Telnet or with a terminal emulator through the access point's serial port.

Table 13-1 lists the access point's diagnostic commands. Click a command in the left column to go to a description of that command's results.

Table 13-1 CLI Diagnostic Commands

Command	Information Displayed
:eap_diag1_on	Authentication progress for client devices authenticating through the access point
:eap_diag2_on	Packet contents of each authentication step for client devices authenticating through the access point
:vxdiag_arpsshow	The ARP table
:vxdiag_checkstack	Task stack on the access point
:vxdiag_hostshow	Remote host list with IP addresses and aliases
:vxdiag_i	Task list on the access point
:vxdiag_ipstatshow	IP statistics
:vxdiag_memshow	Free and allocated memory on the access point
:vxdiag_muxshow	Networking protocols installed on the access point
:vxdiag_routeshow	Current routing information
:vxdiag_tcpstatshow	TCP statistics
:vxdiag_udpstatshow	UDP statistics

**Note**

The `:eap_diag1_on` and `:eap_diag1_on` EAP diagnostic commands are available in firmware versions 11.08 and later. The `:vxdiag_arpshow`, `hostshow`, `ipstatshow`, `muxshow`, `routeshow`, `tcpstatshow`, and `udpstatshow` commands are available in firmware version 11.11T. You can download the latest access point firmware version on Cisco.com at <http://www.cisco.com/public/sw-center/sw-wireless.shtml>.

Entering Diagnostic Commands

Follow these steps to enter diagnostic commands in the CLI:

**Note**

These steps describe opening the CLI with Telnet. If the access point is configured to block Telnet access, follow the instructions in the “Preparing to Use a Terminal Emulator” section on page 2-6 to open the CLI by using a terminal emulator through a serial cable connected to the access point’s serial port.

- Step 1** On your computer’s Start menu, select **Programs > Accessories > Telnet**.
If Telnet is not listed in your Accessories menu, select **Start > Run**, enter **Telnet** in the entry field, and press **Enter**.
- Step 2** When the Telnet window appears, click **Connect**, and select **Remote System**.

**Note**

In Windows 2000, the Telnet window does not contain pull-down menus. To start the Telnet session in Windows 2000, enter **open** followed by the access point’s IP address.

- Step 3** In the Host Name field, enter the access point’s IP address and click **Connect**.
- Step 4** Press **=** to display the access point’s home page.
- Step 5** Enter the command (for example, `:vxdiag_memshow`) and press **Enter**. The command’s diagnostic information appears.

Diagnostic Command Results

This section describes the information displayed on the CLI for the diagnostic commands listed in Table 13-1.

:eap_diag1_on

Use the **:eap_diag1_on** command to display authentication progress for client devices authenticating through the access point. The steps in a successful authentication for a client device named Yakima might look like the following example:

```
EAP: Sending Identity Request
EAP: Received packet from Yakima
EAP: Received Identity Response
EAP: Forwarding packet to RADIUS server
RADIUS: Received packet for client Yakima
RADIUS: Received Challenge Request
RADIUS: Sending EAPOL packet to client
EAP: Received packet from Yakima
EAP: Forwarding packet to RADIUS server
RADIUS: Received packet for client Yakima
RADIUS: Received session timeout request of 60 seconds
RADIUS: Sending EAPOL packet to client
RADIUS: ACCEPT for Yakima
RADIUS: Found Cisco key
RADIUS: Sending EAPOL multicast key
RADIUS: Sending EAPOL session key parameters
EAP: Key set for client Yakima
```

The EAP and RADIUS prefixes show which system process is handling the communication.

Follow the steps in the “Entering Diagnostic Commands” section on page 13-20 to open the CLI and enter the **:eap_diag1_on** command.

:eap_diag2_on

Use the **:eap_diag2_on** command to display the packet contents of each authentication step for client devices authenticating through the access point. The packet contents for one authentication step might look like this example:

```
EAP: Sending Identity Request
00c15730: 01 00 00 28 01 21 00 28 01 00 6e 65 74 77 6f 72 *...(!!(..networ*
00c15740: 6b 69 64 3d 45 41 50 33 2c 6e 61 73 69 64 3d 45 *kid=EAP3,nasid=E*
00c15750: 41 50 33 2c 70 6f 72 74 69 64 3d 30 *AP3,portid=0....*
```

The first group of characters in the packet contents (*00c15730*, for example) is the hexadecimal address of the memory buffer that contains the packet. The middle group of characters (*01 00 00 28 01 21 00 28 01 00 6e 65 74 77 6f 72*, for example) is the packet contents in hexadecimal format. The last group of characters (**...(!!(..networ**, for example) is an ASCII representation of the packet contents.

For information on interpreting the content of packets sent between the access point and the RADIUS server, refer to the Internet Society's *RFC 2865*. This document is available at <http://www.armware.dk/RFC/rfc/rfc2865.html> as well as on many other websites. The IEEE's 802.1X authentication standard helps define the content of packets sent between client devices and the access point and is available to IEEE members at <http://www.ieee.org>.

Follow the steps in the “Entering Diagnostic Commands” section on page 13-20 to open the CLI and enter the **:eap_diag2_on** command.

:vxdiag_arpshow

Use the **:vxdiag_arpshow** command to display the access point's ARP table. The ARP table might look like the following example:

```
LINK LEVEL ARP TABLE
destination      gateway          flags  Refcnt  Use Interface
-----
10.84.139.129    00:05:31:d3:c0:9  405    1        0      emac0
-----
```

These are descriptions for each column in the ARP table:

- Destination—IP address of the host entry
- Gateway—MAC address of the destination

- Flags—see Table 13-2 for a list of flags

Table 13-2 Flag Definitions

Flag Value	Definition
0x1	Route is usable.
0x2	Destination is a gateway.
0x4	Host of specific routing entry.
0x8	Host or net is unreachable.
0x10	Created dynamically (by redirect).
0x20	Modified dynamically (by redirect).
0x40	Message confirmed.
0x80	Subnet mask is present.
0x100	Generate new routes on use.
0x200	External daemon resolves name.
0x400	Generated by ARP.
0x800	Manually added (static).
0x1000	Just discard packets (during updates).
0x2000	Modified by management protocol.
0x4000	Protocol-specific routing flag.
0x8000	Protocol-specific routing flag.

- Refcnt—the number of hosts referencing this address
- Use—number of packets forwarded
- Interface—one of four possible interfaces:
 - *emac0* for Ethernet
 - *awc0* for internal radio
 - *awc1* for external radio
 - *lo0* for internal loopback

Follow the steps in the “Entering Diagnostic Commands” section on page 13-20 to open the CLI and enter the **:vxdiag_arpshow** command.

:vxdiag_checkstack

Use the **:vxdiag_checkstack** command to display a summary of the stack activity for each access point task. A portion of the task stack might look like this example:

NAME	ENTRY	TID	SIZE	CUR	HIGH	MARGIN
tExcTask	0x00001a1fd0	fd4e80	7984	224	960	7024
tSysIntegrit	0x000001b188	a3b1c0	16368	720	1176	15192
tLogEventMgr	0x00000fb0ac	fd22d8	16368	2136	3616	12752
tShell	0x0000041da8	a2eb78	19320	640	2712	16608
tTelnetd	0x000002e220	a32d90	16368	376	1472	14896
tTelnetOutTa	0x000002e7fc	993da0	16368	720	1800	14568
tTelnetInTas	0x000002e858	98fb88	16368	1416	2376	13992

These are the descriptions of the information in each column:

- Name—name of the task
- Entry—entry point; the top-level function of the task
- TID—task identifier; the task control block
- Size—stack size in bytes
- CUR—current number of bytes of stack in use
- High—highest number of bytes of stack which have been in use
- Margin—the difference between the stack size and the highest number of bytes which have been in use

Follow the steps in the “Entering Diagnostic Commands” section on page 13-20 to open the CLI and enter the **:vxdiag_checkstack** command.

:vxdiag_hostshow

Use the **:vxdiag_hostshow** command to display remote hosts and their IP addresses and aliases. The remote host information might look like this example:

Clock: 96470 sec

hostname	ttl	inet address	aliases
-----	---	-----	-----
localhost	0	127.0.0.1	
10.84.139.161	7273	10.84.139.161	
10.84.139.136	7273	10.84.139.136	
10.84.139.138	7273	10.84.139.138	
10.84.139.167	7273	10.84.139.167	
10.84.139.160	7273	10.84.139.160	
10.84.139.137	7273	10.84.139.137	
AP_North.cisco.com	93073	10.84.139.135	
10.84.139.164	7273	10.84.139.164	
10.84.139.169	7274	10.84.139.169	
10.84.139.141	97062	10.84.139.141	

These are descriptions for the information in each column:

- Hostname—Domain name of the host, if available; otherwise, same as the Inet address
- TTL—time-to-live
- Inet address—IP address of the host
- Aliases—List of additional names, other than the hostname, that refer to the Inet address

Follow the steps in the “Entering Diagnostic Commands” section on page 13-20 to open the CLI and enter the **:vxdiag_hostshow** command.

:vxdiag_i

Use the **:vxdiag_i** command to display a list of current tasks on the access point. A portion of the access point's task list display might look like this example:

NAME	ENTRY	TID	PRI	STATUS	PC	SP	ERRNO	DELAY
tExcTask	1a1fd0	fd4e80	0	PEND	1d9aac	fd4da0	3006b	0
tSysIntegrilb188		a3b1c0	0	SUSPEND	1c06ac	a3aef0	0	0
tLogEventMgfb0ac		fd22d8	1	PEND	1bcda8	fd1a80	0	0
tShell	41da8	a2eb78	1	PEND	1bcda8	a2e8f8	9	0
tTelnetd	2e220	a32d90	2	PEND	1bcda8	a32c18	0	0
tTelnetOutT2e7fc		993da0	2	PEND	1bcda8	993ad0	0	0
tTelnetInTa2e858		98fb88	2	PEND	1bcda8	98f600	3d0002	0
tBrowser	1351c8	a0d978	5	READY	1c2014	a0c4b8	3d0004	0
tIdleConsold274c		98b970	10	PEND	1bcda8	98b820	0	0
tThttpd	b435c	a5b3d8	45	PEND	1bcda8	a5b138	6b0003	0
tSNMPD	106fd8	b1eb80	46	PEND+T	1bcda8	b1d5b0	3d0004	1968

These are the descriptions of the information in each column:

- Name—name of the task
- Entry—entry point; the top-level function of the task
- TID—task identifier; the task control block
- PRI—task priority; a low number means a high priority
- Status—status of the task; five statuses are possible:
 - Pend—The task is in an inactive waiting state.
 - Pend+T—The task is waiting, but it has a timeout value for the length of time it will wait for an external event to wake the task and start it.
 - Suspend—The task will not begin until some external event occurs.
 - Ready—The task is ready to run.
 - Delay—The task issued a delay command and will not run until the delay time elapses.
- PC—program counter; a memory address of the task
- SP—stack pointer; another memory address of the task
- ERRNO—error number; the latest error reported by any function called by the task

- Delay—delay interval in system clock-ticks (1/52 second) that must elapse before the task runs

Follow the steps in the “Entering Diagnostic Commands” section on page 13-20 to open the CLI and enter the **:vxdiag_i** command.

:vxdiag_ipstatshow

Use the **:vxdiag_ipstatshow** command to display IP statistics for the access point. The IP statistics might look like the following example:

```
total 5760
badsum      0
tooshort    0
toosmall    0
badhlen     0
badlen      0
infragments 0
fragdropped 0
fragtimeout 0
forward     0
cantforward 0
redirectsent 0
unknownprotocol 0
nobuffers   0
reassembled 0
outfragments 0
noroute     0
```

These are descriptions of each IP statistic:

- Total—the total number of packets received
- Badsum—number of packets received with bad checksums
- Tooshort—number of packets received that were shorter than the expected length
- Toosmall—number of packets received that did not have enough data
- Badhlen—number of packets received with IP header length less than the packet data size
- Badlen—number of packets received with IP length less than the IP header length
- Infragments—number of packets received that were fragmented

- **Fragdropped**—number of fragmented packets received that were dropped
- **Fragtimeout**—number of fragmented packets received that timed out
- **Forward**—number of packets forwarded
- **Cantforward**—number of packets received for an unreachable destination
- **Redirectsent**—number of packets forwarded in the same subnet
- **Unknownprotocol**—number of packets received with unknown protocol information
- **Nobuffers**—number of packets dropped due to unavailable buffers
- **Reassembled**—number of packets reassembled successfully
- **Outfragments**—number of output fragments created
- **Noroute**—number of packets discarded due to no route available

Follow the steps in the “Entering Diagnostic Commands” section on page 13-20 to open the CLI and enter the **:vxdiag_ipstatshow** command.

:vxdiag_memshow

Use the **:vxdiag_memshow** command to display information on the access point’s free and allocated memory. The access point’s current memory information might look like the following example:

status	bytes	blocks	avg block	max block
current				
free	7386392	476	15517	7296288
alloc	6738808	10837	621	-
cumulative				
alloc	13483152	126889	106	-

These are descriptions for each information column:

- **Status**—the memory statuses described in the table, including current free memory, current allocated memory, and cumulative allocated memory, which is the total bytes and blocks of memory ever allocated by the access point
- **bytes**—the memory for each status described in bytes
- **blocks**—the memory for each status described in contiguous blocks; indicates the level of fragmentation in the access point’s memory

- avg block—the average block size; simply put, the number in the bytes column divided by the number in the blocks column
- max block—the maximum contiguous memory block available

Follow the steps in the “Entering Diagnostic Commands” section on page 13-20 to open the CLI and enter the **:vxdiag_memshow** command.

:vxdiag_muxshow

Use the **:vxdiag_muxshow** command to display all the networking protocols installed on the access point. The list of installed protocols might look like the following example:

```
Device: emac Unit: 0
Description: PPC405GP Ethernet Media Access Controller Enhanced Network Driver
Protocol: AWC Packet Router      Type: 257      Recv 0x5ad0c   Shutdown 0x5fbd0
Protocol: Cisco Discovery Protocol (CDP)      Type: 8192      Recv 0x4f2c0
Shutdown 0x0
Protocol: AWC DDP Protocol      Type: 34605      Recv 0x6986c   Shutdown 0x6a728
Protocol: IP 4.4 ARP      Type: 2054      Recv 0x2732c   Shutdown 0x275ec
Protocol: IP 4.4 TCP/IP Type: 2048      Recv 0x2732c   Shutdown 0x27524
Device: awc Unit: 0
Description: Aironet A504-Family Enhanced Network Driver
Protocol: AWC DDP Protocol      Type: 34605      Recv 0x6986c   Shutdown 0x6a728
Protocol: 802.1X Protocol      Type: 34958      Recv 0x9adc4   Shutdown 0x9e5a0
Protocol: AWC WNMP MAC-Level Control      Type: 34689      Recv 0x118af4   Shutdown
0x118e9c
Protocol: AWC 802.11 MAC-Level Control      Type: 57841      Recv 0x6c258   Shutdown
0x6c5dc
Protocol: AWC 802.11 MAC-Level Management      Type: 57840      Recv 0x6abf0
Shutdown 0x6c580
Protocol: AWC Packet Router      Type: 511      Recv 0x5ad0c   Shutdown 0x5fbd0
Device: rptr Unit: 1
Description: Aironet 802.11 Bridge Driver
Protocol: AWC Packet Router      Type: 257      Recv 0x5ad0c   Shutdown 0x5fbd0
Protocol: AWC DDP Protocol      Type: 34605      Recv 0x6986c   Shutdown 0x6a728
Device: rptr Unit: 2
```

Follow the steps in the “Entering Diagnostic Commands” section on page 13-20 to open the CLI and enter the **:vxdiag_muxshow** command.

:vxdiag_routeshow

Use the **:vxdiag_routeshow** command to display current routing information for the access point. The routing information might look like the following example:

ROUTE NET TABLE					
destination	gateway	flags	Refcnt	Use	Interface

0.0.0.0	10.84.139.129	3	1	1932	emac0
10.84.139.128	10.84.139.141	101	0	0	emac0

ROUTE HOST TABLE					
destination	gateway	flags	Refcnt	Use	Interface

127.0.0.1	127.0.0.1	5	0	696	lo0

These are descriptions for each column in the route net and route host tables:

- Destination—IP address of host to which access point is to be routed
- Gateway—IP address of host for forwarding packets not in the access point's subnet
- Flags—see Table 13-2 for a list of flags
- Refcnt—the number of hosts referencing this address
- Use—number of packets forwarded
- Interface—one of four possible interfaces:
 - *emac0* for Ethernet
 - *awc0* for internal radio
 - *awc1* for external radio
 - *lo0* for internal loopback

Follow the steps in the “Entering Diagnostic Commands” section on page 13-20 to open the CLI and enter the **:vxdiag_routeshow** command.

:vxdiag_tcpstatshow

Use the :vxdiag_tcpstatshow command to display Transmission Control Protocol (TCP) statistics for the access point. The TCP statistics might look like this example:

TCP:

```
3370 packets sent
    1576 data packets (714752 bytes)
    3 data packets (1613 bytes) retransmitted
    1252 ack-only packets (1 delayed)
    0 URG only packet
    1 window probe packet
    0 window update packet
    538 control packets
3327 packets received
    1564 acks (for 710621 bytes)
    23 duplicate acks
    0 ack for unsent data
    824 packets (189251 bytes) received in-sequence
    8 completely duplicate packets (2562 bytes)
    0 packet with some dup. data (0 byte duped)
    74 out-of-order packets (0 byte)
    0 packet (0 byte) of data after window
    0 window probe
    85 window update packets
    0 packet received after close
    0 discarded for bad checksum
    0 discarded for bad header offset field
    0 discarded because packet too short
63 connection requests
415 connection accepts
477 connections established (including accepts)
477 connections closed (including 410 drops)
0 embryonic connection dropped
1378 segments updated rtt (of 1399 attempts)
2 retransmit timeouts
    0 connection dropped by rexmit timeout
1 persist timeout
0 keepalive timeout
    0 keepalive probe sent
    0 connection dropped by keepalive
63 pcb cache lookups failed
```

Follow the steps in the “Entering Diagnostic Commands” section on page 13-20 to open the CLI and enter the :vxdiag_tcpstatshow command.

:vxdiag_udpstatshow

Use the **:vxdiag_udpstatshow** command to display User Datagram Protocol (UDP) statistics for the access point. The UDP statistics might look like this example:

```
UDP:
    9244 total packets
    9227 input packets
    17 output packets
    0 incomplete header
    0 bad data length field
    0 bad checksum
    9211 broadcasts received with no ports
    0 full socket
    16 pcb cache lookups failed
    0 pcb hash lookup failed
```

Follow the steps in the “Entering Diagnostic Commands” section on page 13-20 to open the CLI and enter the **:vxdiag_udpstatshow** command.

Tracing Packets

Use the packet tracing feature to view packets sent and received by the access point and by other wireless devices on your network. You can view packets sent to and received from a single wireless device or several wireless devices, or you can view all the packets sent and received through the access point’s Ethernet and radio ports.

The IEEE’s 802.1X authentication standard helps define the content of packets and is available to IEEE members at <http://www.ieee.org>.

For information on filtering packets, see the “Radio Configuration” section on page 3-8.

Reserving Access Point Memory for a Packet Trace Log File

You can save packet traces in a log file that you view or save, or you can view packets on the access point command-line interface without storing the traces in a log file. Use the instructions in this section to reserve access point memory for

a packet trace log file. Use the instructions in the “Tracing Packets for Specific Devices” section on page 13-33 and the “Tracing Packets for Ethernet and Radio Ports” section on page 13-34 to select devices and ports to be traced.

Follow these steps to reserve access point memory for a packet trace log file:

-
- Step 1** Use the Event Handling Setup page to enter instructions for the size of the packets you want to monitor and the amount of memory the access point should set aside for packet data. Follow this link path to the Event Handling Setup page:
- a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **Event Handling** under Event Log.
- Step 2** Enter the number of bytes the access point should store for each packet in the Maximum number of bytes stored per Alert packet entry field. If you want to see the entire contents of each packet, enter **1600**; if you want to see only the packet header, enter **64**.
- Step 3** Enter the number of bytes of memory the access point should use for packet tracing in the Maximum memory reserved for Detailed Event Trace Buffer (bytes) entry field. If you want to create a detailed packet trace, for example, enter **1000000**; if you need a simple, less-detailed packet trace, for example, enter **100000**.
- Step 4** Click **OK**. The access point reboots.

Now you need to enter settings for the wireless devices or network interfaces for which you want to trace packets. Follow the steps in the “Tracing Packets for Specific Devices” section on page 13-33 or the “Tracing Packets for Ethernet and Radio Ports” section on page 13-34 to select devices and ports to be monitored.

Tracing Packets for Specific Devices

Follow these steps to select specific devices for which you want to trace packets:

-
- Step 1** Browse to the access point’s Association Table. You can reach the Association Table by clicking **Current Associations** on the Summary Status page or by clicking the gray **Associations** button at the top of most management system pages.

- Step 2** Find the wireless device for which you want to trace packets and click the device's MAC address. The device's Station page appears.
- Step 3** On the device's Station page, click the **alert** checkbox in the To Station header to trace packets sent to the device. Click the **alert** checkbox in the From Station header to trace packets the device sends.

**Note**

Copying packets into access point memory slows the access point's performance. When you finish tracing packets, deselect the alert checkboxes on the Station pages.

If you want the access point to trace packets all the time, reduce the impact on performance by selecting **Record** for the External Information setting on the Event Handling Setup page and select **Port Information** on the Event Display Setup page for the "Severity Level at which to display events immediately on the console" setting. With this configuration, the access point records packets in a log file but does not spend time instantly displaying packets on the CLI.

- Step 4** Click Refresh. Repeat these steps for each device for which you want to trace packets. The MAC addresses of devices you are tracing appear in red in the Association Table.

If you are ready to view packet data, skip to the "Viewing Packet Trace Data" section on page 13-35. If you want to trace all the packets sent through the access point's Ethernet and radio ports, follow the instructions in the "Tracing Packets for Ethernet and Radio Ports" section on page 13-34.

Tracing Packets for Ethernet and Radio Ports

Follow these steps to set up the access point's Ethernet or radio ports for packet tracing:

- Step 1** To trace all the packets sent and received through the access point's Ethernet or radio ports, browse to the Network Ports page. Browse to the Network Ports page by clicking **Current Associations** on the Summary Status page or by clicking the gray **Network** button at the top of most management system pages.

- Step 2** To trace packets sent or received through the access point's Ethernet port, click **Ethernet** in the yellow header row. To trace packets sent or received through the access point's radio port, click **AP Radio** in the yellow header row. The Ethernet Port or AP Radio Port page appears.
- Step 3** Click the **alert** checkbox in the Receive header to trace packets received through the Ethernet or radio port. Click the **alert** checkbox in the Transmit header to trace packets sent through the Ethernet or Radio port.

**Note**

Copying packets into access point memory slows the access point's performance. When you finish tracing packets, deselect the alert checkboxes on the Station pages.

If you want the access point to trace packets all the time, reduce the impact on performance by selecting **Record** for the External Information setting on the Event Handling Setup page and select **Port Information** on the Event Display Setup page for the "Severity Level at which to display events immediately on the console" setting. With this configuration, the access point records packets in a log file but does not spend time instantly displaying packets on the CLI.

- Step 4** Click **Refresh**. The network interface you are tracing appears in red on the Summary Status, Setup, and Network Ports pages.
- Step 5** Follow the steps in the "Viewing Packet Trace Data" section on page 13-35 to view the traced packets in a log file or on the CLI.

Viewing Packet Trace Data

If you store traced packets in a log file, you can view or save the file. If you do not store traced packets, you can view the packets in real time on the access point CLI.

Packets Stored in a Log File

Follow these steps to view traced packets stored in a log file:

-
- Step 1** Browse to the Event Handling Setup page. Follow this link path to the Event Handling Setup page:
- a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **Event Handling** under Event Log.
- Step 2** Click **Headers Only** to view only the packet headers; click **All Data** to view all the collected packet information.
- Step 3** A File Download window appears asking if you want to save the [access point name]_trace.log file or open it. Choose to save or open the file and click **OK**.

A portion of the Headers Only packet trace file might look like this example:

```
===Beginning of AP_North Detailed Trace Log===
04:46:14 +17174.384615 Station Alert: 00:01:64:43:ef:41Aironet:40:6f:e6Aironet:40:6f:e6
0x0000
04:47:37 + 83.326923 Station Alert: 00:01:64:43:ef:41Aironet:40:6f:e6Aironet:36:14:5a
0x0000
04:49:06 + 88.307692 Station Alert: 00:01:64:43:ef:41Aironet:40:6f:e6broadcastARP
04:49:06 + 0.000000 Station Alert: 00:05:31:d3:c0:0900:01:64:43:ef:41ARP
04:49:06 + 0.000000 Station Alert: 00:01:64:43:ef:41Aironet:40:6f:e600:05:31:d3:c0:09IP
IPv4 UDP ID=0x14f2 totalLen=96 10.84.139.164 -> ne-wins.cisco.com
04:49:06 + 0.230769 Station Alert: 00:05:31:d3:c0:0900:01:64:43:ef:41IP IPv4 UDP
ID=0xb0b4 totalLen=90 ne-wins.cisco.com -> 10.84.139.164
04:49:06 + 0.019231 Station Alert: 00:01:64:43:ef:41Aironet:40:6f:e600:05:31:d3:c0:09IP
IPv4 UDP ID=0x14f3 totalLen=96 10.84.139.164 -> ne-wins.cisco.com
04:49:06 + 0.192308 Station Alert: 00:05:31:d3:c0:0900:01:64:43:ef:41IP IPv4 UDP
ID=0xb2b4 totalLen=90 ne-wins.cisco.com -> 10.84.139.164
===End of AP_North Detailed Trace Log===
```

A portion of the All Data packet trace file might look like this example:

```
===Beginning of AP_North Detailed Trace Log===
04:46:14 +17174.384615 Station Alert:
00:01:64:43:ef:41[Aironet]00:40:96:40:6f:e6[Aironet]00:40:96:40:6f:e6 0x0000
00 4a 40 81 00 40 96 40 6f e6 00 01 64 43 ef 41 01 7f 00 04 5f 00 00 40 96 40 6f e6 00 00
00 00 00 00 00 00 00 00 0a 54 8b a4 00 00 44 57 49 4c 4c 2d 49 42 4d 2d 57 32 4b 00 00 00
00 00 00 00 00 00 |.J@..@.o...dC.A..._..@.o.....T....JCOOL-IBM-W2K.....|
04:47:37 + 83.326923 Station Alert:
00:01:64:43:ef:41[Aironet]00:40:96:40:6f:e6[Aironet]00:40:96:36:14:5a 0x0000
```



```

00 4a 40 81 00 40 96 36 14 5a 00 01 64 43 ef 41 01 7f 00 04 5f 00 00 40 96 40 6f e6 00 00
00 00 00 00 00 00 00 00 00 00 0a 54 8b a4 00 00 44 57 49 4c 4c 2d 49 42 4d 2d 57 32 4b 00 00 00
00 00 00 00 00 00 00 |.J@..@.6.Z..dC.A..._...@.@o.....T....JCOOL-IBM-W2K.....|
===End of AP_North Detailed Trace Log===

```

Packets Displayed on the CLI

To view packets displayed on the access point CLI, follow the instructions in the “Using the Command-Line Interface” section on page 2-5 to open the CLI. The access point displays the packets at the bottom of the screen.

Checking the Top Panel Indicators

If your access point is not communicating, check the three indicators on the top panel. The indicators report the unit’s status. Figure 13-11 shows the indicators on an access point with a plastic case, and Figure 13-12 shows the indicators on an access point with a metal case. Table 13-3 lists the meanings of the indicator signals.

Figure 13-11 Indicator Lights on Access Point with Plastic Case

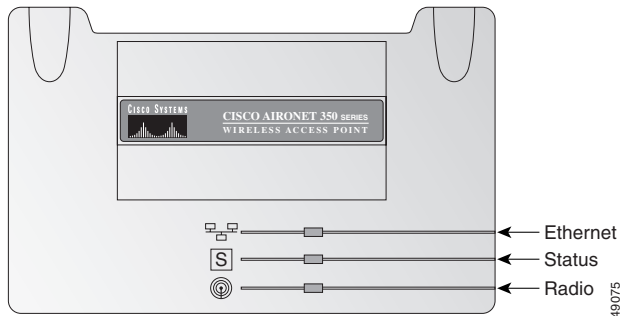
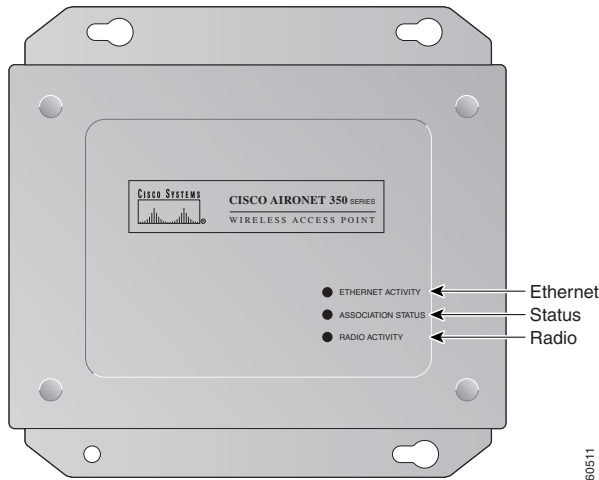


Figure 13-12 Indicator Lights on Access Point with Metal Case

- The Ethernet indicator signals traffic on the wired LAN, or Ethernet infrastructure. This indicator blinks green when a packet is received or transmitted over the Ethernet infrastructure.
- The status indicator signals operational status. Blinking green indicates that the access point is operating normally but is not associated with any wireless devices. Steady green indicates that the access point is associated with a wireless client.

For repeater access points, blinking 50% on, 50% off indicates the repeater is not associated with the root access point; blinking 7/8 on, 1/8 off indicates that the repeater is associated with the root access point but no client devices are associated with the repeater; steady green indicates that the repeater is associated with the root access point and client devices are associated with the repeater.

- The radio indicator blinks green to indicate radio traffic activity. The light is normally off, but it blinks green whenever a packet is received or transmitted over the access point's radio.

Table 13-3 Top Panel Indicator Signals

Message type	Ethernet indicator	Status indicator	Radio indicator	Meaning
Association status	–	Steady green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the unit's SSID and WEP settings.
Operational	–	Steady green	Blinking green	Transmitting/receiving radio packets.
	Blinking green	Steady green	–	Transmitting/receiving packets.
	–	Steady green	Blinking amber	Maximum retries or buffer full occurred on the radio.
Error/warning	Blinking amber	Steady green	–	Transmit/receive errors.
	Blinking red	–	–	Ethernet cable is disconnected (340 series only).
	–	Blinking amber	–	General warning.
Failure	Steady red	Steady red	Steady red	Firmware failure; disconnect power from the unit and reapply power.
Firmware upgrade	–	Steady red	–	Unit is loading new firmware.

Finding an Access Point by Blinking the Top Panel Indicators

If you need to find the physical location of a particular access point, you can put the top panel indicators into blinking mode. Follow these instructions to blink the access point's top panel indicators:

-
- Step 1** Browse to the access point's Cisco Services Setup page:
- a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **Cisco Services**.
- Step 2** Select **Enabled** for the Locate unit by flashing LEDs option.
- Step 3** Click **Apply**. The access point's top panel indicators blink amber in unison.
- Step 4** To make the indicators stop blinking and return to normal operation, select **Disabled** for the Locate unit by flashing LEDs option, and click **Apply**.
-

Checking Basic Settings

Mismatched basic settings are the most common causes of lost connectivity with wireless clients. If the access point does not communicate with client devices, check the following settings.

SSID

Wireless clients attempting to associate with the access point must use the same SSID as the access point. The default SSID is tsunami.

WEP Keys

The WEP key you use to transmit data must be set up exactly the same on your access point and any wireless devices with which it associates. For example, if you set WEP Key 3 on your wireless LAN adapter to 0987654321 and select it as

the transmit key, you must also set WEP Key 3 on the access point to exactly the same value. The access point does not need to use Key 3 as its transmit key, however.

**Note**

If you use Network-EAP as the authentication type, you must select key 1 as the access point's transmit key. The access point uses the WEP key you enter in key slot 1 to encrypt multicast data signals it sends to EAP-enabled client devices. Because the access point transmits the WEP key used for multicast messages to the EAP-enabled client device during the EAP authentication process, that key does not have to appear in the EAP-enabled device's WEP key list. The access point uses a dynamic WEP key to encrypt unicast messages to EAP-enabled clients.

Refer to the "Setting Up WEP" section on page 7-9 for instructions on setting the access point's WEP keys.

EAP Authentication Requires Matching 802.1X Protocol Drafts

**Note**

This section applies to wireless networks set up to use LEAP. If you do not use LEAP on your wireless network, you can skip this section.

Wireless client devices use Extensible Authentication Protocol (EAP) to log onto a network and generate a dynamic, client-specific WEP key for the current logon session. If your wireless network uses WEP without EAP, client devices use the static WEP keys entered in the Aironet Client Utilities.

If you use Network-EAP authentication on your wireless network, your client devices and access points must use the same 802.1X protocol draft. For example, if the radio firmware on the client devices that will associate with an access point or bridge is 4.16, then the access point or bridge should be configured to use Draft 8 of the 802.1X protocol. Table 13-4 lists firmware versions for Cisco Aironet products and the draft with which they comply.

Table 13-4 802.1X Protocol Drafts and Compliant Client Firmware

Firmware Version	Draft 7	Draft 8	Draft 10
PC/PCI cards 4.13	—	x	—
PC/PCI cards 4.16	—	x	—
PC/PCI cards 4.23	—	x	—
PC/PCI cards 4.25 and later	—	—	x
WGB34x/352 8.58	—	x	—
WGB34x/352 8.61 or later	—	—	x
AP34x/35x 11.05 and earlier	—	x	—
AP34x/35x 11.06 and later ¹	—	x	x
BR352 11.06 and later ¹	—	x	x

1. The default draft setting in access point and bridge firmware version 11.06 and later is Draft 10.

**Note**

Draft standard 8 is the default setting in firmware version 11.05 and earlier, and it might remain in effect when you upgrade the firmware to version 11.06 or later. Check the setting on the Authenticator Configuration page in the management system to make sure the best draft standard for your network is selected.

Use the Authenticator Configuration page to select the draft of the 802.1X protocol the access point's radio should use. Follow these steps to set the draft for your access point:

- Step 1** Browse to the Authenticator Configuration page in the access point management system.
- On the Summary Status page, click **Setup**.
 - On the Setup page, click **Security**.
 - On the Security Setup page, click **Authentication Server**.

- Step 2** Use the 802.1X Protocol Version (for EAP authentication) pull-down menu to select the draft of the 802.1X protocol the access point's radio should use. Menu options include:
- Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting.
 - Draft 8—Select this option if LEAP-enabled client devices that associate with this access point use radio firmware versions 4.13, 4.16, or 4.23.
 - Draft 10—This is the default setting in access point firmware versions 11.06 and later. Select this option if client devices that associate with this access point use Microsoft Windows XP EAP authentication or if LEAP-enabled client devices that associate with this bridge use radio firmware version 4.25 or later.
- Step 3** Click **Apply** or **OK** to apply the setting. The access point reboots.
-

Resetting to the Default Configuration

If you forget the password that allows you to configure the access point, you might need to completely reset the configuration. Follow the steps below to delete the current configuration and return all access point settings to the factory defaults.

Steps for Firmware Versions 11.07 or Later

Follow the steps in this section if your access point is running firmware version 11.07 or later.



Note

The following steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID. If you do not need to reset the entire configuration, use the Configuration Reset buttons on the System Configuration Setup page in the web-browser interface. Consult the “Resetting the Configuration” section on page 9-16 for more information on the reset buttons in the web-browser interface.

Step 1 Use a straight-through cable with 9-pin male to 9-pin female connectors to connect the COM 1 or COM 2 port on your computer to the RS-232 port on the access point.

Step 2 Open a terminal-emulation program on your computer.



Note These instructions describe HyperTerminal; other programs are similar.

Step 3 In the Connection Description window, enter a name and select an icon for the connection and click **OK**.

Step 4 In the Connect To window, select the port to which the cable is connected and click **OK**.

Step 5 In the Port Settings window, enter the following settings:

- **9600** baud,
- **8** data bits,
- **No** parity,
- **1** stop bit, and
- **Xon/Xoff** flow control

Step 6 Click **OK**, and press **Enter**.

Step 7 When the Summary Status screen appears, reboot the access point by unplugging the power connector and then plugging it back in.

Step 8 When the access point reboots and the Summary Status screen reappears, type **:resetall**, and press **Enter**.

Step 9 Type **yes**, and press **Enter** to confirm the command.



Note The **resetall** command is valid for only 2 minutes immediately after the access point reboots. If you do not enter and confirm the resetall command during that 2 minutes, reboot the access point again.

Step 10 After the access point reboots and the Express Setup screen appears, reconfigure the access point by using the terminal emulator or an Internet browser.

Steps for Firmware Versions 11.06 or Earlier

Follow the steps in this section if your access point is running firmware version 11.06 or earlier.

**Note**

The following steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID. If you do not need to reset the entire configuration, use the Configuration Reset buttons on the System Configuration Setup page in the web-browser interface. Consult the “Resetting the Configuration” section on page 9-16 for more information on the reset buttons in the web-browser interface.

Determining the Boot-Block Version

The steps you follow to reconfigure the access point depend on the version of the access point’s boot block. Follow these steps to find out which boot block version is on your access point:

Step 1 Open a Telnet session to the access point.

**Note**

You can also use these instructions while communicating with the access point through the console port or with an SNMP manager. Skip to Step 3 if you use an SNMP manager.

Step 2 Type **:cmd** and press **Enter** to switch from text-browser mode to SNMP mode.

Step 3 Type **bootblockVersion** and press **Enter**. Text appears with information about the system. If your access point’s boot block version is 1.01, the text might look like this:

```
OID: iso.org.dod.internet.private.enterprises.aironet.awcVx.awcSystem.  
bootblockVersion  
Value [RO]: 1.01
```

Step 4 Type **exit** and press **Enter** to return to text-browser mode.

- Step 5** If your boot block version is 1.01 or earlier, follow the instructions in the “Reconfiguration Steps for Boot Block Version 1.01 or Earlier” section on page 13-46. If your boot block version is 1.02 or later, follow the instructions in the “Reconfiguration Steps for Boot Block Version 1.02 or Later” section on page 13-48.
-

Reconfiguration Steps for Boot Block Version 1.01 or Earlier

Follow these steps to reconfigure your access point if the boot block version on your access point is version 1.01 or earlier and the firmware version on your access point is 11.06 or earlier. To find which boot block version is on your access point, follow the steps in the “Determining the Boot-Block Version” section on page 13-45.



Caution

Failure to follow these instructions correctly can result in a nonoperational access point that must be returned to the factory. If your access point stops working after you attempt this procedure, contact Cisco TAC for assistance.

- Step 1** Use a straight-through cable with 9-pin male to 9-pin female connectors to connect the COM 1 or COM 2 port on your computer to the RS-232 port on the access point.
- Step 2** Open a terminal-emulation program on your computer.



Note

These instructions describe HyperTerminal; other programs are similar.

- Step 3** In the Connection Description window, enter a name and select an icon for the connection and click **OK**.
- Step 4** In the Connect To window, select the port to which the cable is connected and click **OK**.
- Step 5** In the Port Settings window, make the following settings: **9600** baud, **8** data bits, **No** parity, **1** stop bit, and **Xon/Xoff** flow control.
- Step 6** Click **OK** and press **Enter** three times.

- Step 7** When the Summary Status screen appears, reboot the access point by unplugging the power connector and then plugging it back in, or by pressing **Ctrl-X**.
- Step 8** When the message “Type <esc> within 5 seconds for menu” appears, press **Esc**.
- Step 9** Write down the list of files for future reference.

**Caution**

Perform the next six steps carefully to avoid accidentally deleting the installation key files or the firmware files. You must carefully note the file selection letters, because they change during the following steps. If you forget to copy the access point’s installation key file to DRAM in Step 10, or if you do not copy it back to configuration memory in Step 13, your access point will stop functioning.

- Step 10** Copy the access point’s installation key file to the access point’s DRAM by pressing **c** to select **Copy file**, then **1** to select **DRAM**, then the selection letter for the file called *AP Installation Key*.
- Step 11** If the list of configuration files contains a file called *VAR Installation Key*, copy that file to DRAM along with the AP Installation Key. Copy the VAR installation key file to DRAM by pressing **c** to select **Copy file**, then **1** to select **DRAM**, then the selection letter for the file called *VAR Installation Key*.

**Caution**

Make sure you select the Configuration memory bank for formatting in Step 12. If you accidentally format a different memory bank your access point will stop functioning.

- Step 12** Reformat the access point’s configuration memory bank by pressing **!** to select **FORMAT memory bank**, then **2** to select **Config**, then upper-case **Y** to confirm the **FORMAT** command.
- Step 13** Copy the installation key back to the configuration memory bank by pressing **c** to select **Copy file**, then **2** to select **Config**, then the selection letter for the AP Installation Key.
- Step 14** If you copied a VAR installation key to DRAM in Step 11, copy it back to the configuration memory bank by pressing **c** to select **Copy file**, then **2** to select **Config**, then the selection letter for the file *VAR Installation Key*. If the access point does not have a VAR installation key file, skip to Step 15.

- Step 15** Run the access point firmware by pressing **r** to select **Run**, then the selection letter for the firmware file which is displayed. The message “Inflating [firmware file name]” appears while the access point starts the firmware.
- Step 16** When the Express Setup screen appears, begin reconfiguring the access point using the terminal emulator or an Internet browser.
-

Reconfiguration Steps for Boot Block Version 1.02 or Later

Follow these steps to reconfigure your access point if the boot block version on your access point is version 1.02 or later and the firmware version on your access point is 11.06 or earlier. To find which boot block version is on your access point, follow the steps in the “Determining the Boot-Block Version” section on page 13-45.



Caution

Failure to follow these instructions correctly can result in a nonoperational access point that must be returned to the factory. If your access point stops working after you attempt this procedure, contact Cisco TAC for assistance.

- Step 1** Use a straight-through cable with 9-pin male to 9-pin female connectors to connect the COM 1 or COM 2 port on your computer to the RS-232 port on the access point.
- Step 2** Open a terminal-emulation program on your computer.



Note

These instructions describe HyperTerminal; other programs are similar.

- Step 3** In the Connection Description window, enter a name and select an icon for the connection and click **OK**.
- Step 4** In the Connect To window, select the port to which the cable is connected and click **OK**.
- Step 5** In the Port Settings window, make the following settings: **9600** baud, **8** data bits, **No** parity, **1** stop bit, and **Xon/Xoff** flow control.
- Step 6** Click **OK** and press **Enter**.

- Step 7** When the Summary Status screen appears, reboot the access point by pressing **Ctrl-X** or by unplugging the power connector and then plugging it back in.
- Step 8** When the memory files are listed under the heading “Memory:File,” press **Ctrl-W** within 5 seconds to reach the boot block menu.
- Step 9** Write down the list of files for future reference.

**Caution**

Perform the next six steps carefully to avoid accidentally deleting the installation key files or the firmware files. You must carefully note the file selection letters, because they change during the following steps. If you forget to copy the access point’s installation key file to DRAM in Step 10, or if you do not copy it back to configuration memory in Step 13, your access point will stop functioning.

- Step 10** Copy the access point’s AP Installation Key to the access point’s DRAM by pressing **c** to select **Copy file**, then **1** to select **DRAM**, then the selection letter for the file *AP Installation Key*.
- Step 11** If the list of configuration files contains a file called *VAR Installation Key*, you must copy that file to DRAM along with the AP Installation Key file. If the access point does not have a VAR installation key file, skip to Step 12.

**Caution**

If you forget to copy the access point’s VAR installation key file to DRAM in Step 11, or if you do not copy it back to configuration memory in Step 14, your access point will stop functioning.

Copy the VAR Installation Key to DRAM by pressing **c** to select **Copy file**, then **1** to select **DRAM**, then the selection letter for the file *VAR Installation Key*.

- Step 12** Reformat the access point’s configuration memory bank by pressing **Ctrl-Z** to reach the reformat menu. When the menu appears, press **!** to select **FORMAT memory bank**, then **2** to select **Config**, then upper-case **Y** to confirm the **FORMAT** command.

**Caution**

Make sure you select the Configuration memory bank for formatting. If you accidentally format a different memory bank your access point will stop functioning.

- Step 13** Copy the installation key back to the configuration memory bank by pressing **c** to select **Copy file**, then **2** to select **Config**, then the selection letter for the file *AP Installation Key*.
- Step 14** If you copied a VAR installation key to DRAM in Step 11, copy it back to the configuration memory bank by pressing **c** to select **Copy file**, then **2** to select **Config**, then the selection letter for the file *VAR Installation Key*. If the access point does not have a VAR installation key file, skip to Step 15.
- Step 15** Run the access point firmware by pressing **r** to select **Run**, then the selection letter for the firmware file that is displayed. The message “Inflating [firmware file name]” appears while the access point starts the firmware.
- Step 16** When the Express Setup screen appears, begin reconfiguring the access point using the terminal emulator or an Internet browser.
-



Menu Tree

This section provides a menu tree for the Access Point management pages. The pages are organized the same way for all interfaces. Submenus are indicated as subordinate levels. Information inside parentheses is the title of the page to which the menu option selected directs you to.

Figures A-1 through A-6 show the organization for the management system's home page (Summary Status) and sub-pages.

Figure A-1 Summary Status Home Page Menu Map

Summary Status

- Current Associations > (Association Table)
 - Clients > (Association Table)
 - Repeaters > (Association Table)
 - Bridges > (Association Table)
 - Aps > (Association Table)
- Recent Events > (Event Log)
- Network Ports > Network Ports
 - Ethernet > (Ethernet Port)
 - Set Properties > (Ethernet Hardware Setup)
 - AP Radio > (AP Radio Port)
 - Set Properties > (AP Radio Hardware Setup)
 - SSID more > (AP Radio Service Sets Setup)
 - Restrict Searched Channels (AP Radio ... Channels Setup)
 - VLAN Setup > (VLAN Setup)
 - Radio Data Encryption (WEP) > (AP Radio Data Encryption Setup)
 - VLAN Setup > (VLAN Setup)
 - VLAN Summary Status

Figure A-2 Summary Status Map Menu Tree

[Help] > (Help) [Network Map] > (Network map)

Summary Status > (Summary Status)
 Association > (Association Table)
 Event Logs > (Event Log)
 Network Ports > (Network Ports)
 Setup > (Setup)

Figure A-3 Summary Status Network Menu Tree

Summary Status Network > (Network Ports)
 Ethernet > (Ethernet Port)
 Set Properties > (Ethernet Hardware)

Figure A-4 Summary Status Associations Menu Tree

Summary Status Associations > (Association Table)
 Network Diagnostics > (Network Diagnostics)
 Radio Diagnostics Tests > (Radio Diagnostics)
 Carrier Test Start

Figure A-5 Summary Status Setup Menu Tree

Summary Status Express Setup > (Express Setup)
 Configuration Server Protocol > (Boot Server Setup)
 Default Gateway > (Routing Setup)
 Radio Service Set ID (SSID) more > (AP Radio Service Sets)
 Optimize Radio Network For Custom > (AP Radio Hardware)
 Service Set ID (SSID) more > (AP Radio Service Sets)
 Radio Channel? Restrict Searched Channels > (AP Radio...Search Channels)
 VLAN Setup > (VLAN Setup)
 VLAN Summary Status (VLAN Summary Status)
 Radio Data Encryption (WEP) > (AP Radio Data Encryption)
 VLAN Setup > (VLAN Setup)
 SNMP Admin. Community > (SNMP Setup)
 Browse Management Information Base (MIB) > (Database Query)

Associations Section

- Display Defaults > (Association Table Filters)
- Address Filters > (Address Filters)
 - Authentication Server > (Authenticator Configuration)
- Protocol Filters > (Protocol Filters Setup)
 - Ethertype Filters > (Ethertype Protocol. Filters)
 - IP Protocol Filters > (IP Protocol Filters)
 - IP Port Filters > (IP Port Filters)
 - Policy Groups > (Policy Groups)
- Quality of Service > (AP Radio Quality of Service)
- Port Assignments > (Port Assignments)
- VLAN > (VLAN Setup)
- Advanced > (Association Table Advanced)
- Service Sets > (AP Radio Service Sets)

Event Log Section

- Display Defaults > (Event Display Setup)
- Event Handling > (Event Handling Setup)
 - Download Detailed Event Tracer Buffer Headers Only
 - Download Detailed Event Tracer Buffer All Data
- Notifications > (Event Notifications Setup)

Services Section

- Console/Telnet > (Console/Telnet Setup)
- Time Server > (Time Server Setup)
- Boot Server > (Boot Server Setup)
- FTP > (FTP Setup)
- Cisco Services > (Cisco Services Setup)
 - Manage Installation Keys > (Manage Installation Keys)
 - Manage System Configuration > (System Configuration Setup)
 - “WARM” RESTART SYSTEM NOW
 - “COLD” RESTART SYSTEM NOW
 - Download Non-Default System Configuration *Except* IP Identity
 - Reset System Factory Defaults *Except* IP Identity
 - Download Non-Default System Configuration
 - Download **All** System Configuration
 - Reset All System Factory Defaults
 - Distribute Firmware to other Cisco Devices > (Distribute Firmware)
 - Hot Standby Management > (Hot Standby)
 - Start Hot Standby Mode
 - Stop Hot Standby Mode
 - Cisco Discovery Protocol (CDP) > (CDP Setup)
 - Fully Update Firmware Through Browser > (Update All Firmware Through Browser)
 - Retrieve All Firmware Files
 - Fully Update Firmware From File Server > (Update All Firmware From File Server)
 - File Server Setup > (FTP Setup)
 - Selectively Update Firmware Through Browser > (Update Firmware.Through Browser)
 - Current Version of System Firmware

- Current Version of Web Pages
- Current Version of Radio Firmware
- Selectively Update Firmware From File Server > (Update Firmware.Through File Server)
 - Current Version of System Firmware
 - Current Version of Web Pages
 - Current Version of Radio Firmware
- File Server Setup > (FTP Setup)
- Routing > (Routing Setup)
- Web Server > (Web Server Setup)
- Security > (Security Setup)
 - Login > (Login)
 - User Manager > (User Manager Setup)
- Change Current User Password > (User Information)
- Authentication Server > (Authentication Server Setup)
- VLAN Setup > (VLAN Setup)
- Radio Data Encryption (WEP) > (AP Radio Data Encryption)
 - VLAN Setup > (VLAN Setup)
- Name Server > (Name Server Setup)
- SNMP > (SNMP Setup)
 - Browse Management Information Base (MIB) > (Database Query)
- Accounting > (Accounting Setup)

Network Ports Section

- Diagnostics > (Network Diagnostics)
 - Radio Diagnostics Tests > (Radio Diagnostics)
 - Carrier Test Start
- Ethernet > (Ethernet Port)
 - Set Properties > (Ethernet Hardware)
- Ethernet Identification > (Ethernet Identification)
- Ethernet Hardware > (Ethernet Hardware)
- Ethernet Filters > (Ethernet Protocol Filters)
 - Ethertype > (Ethertype Protocol Filters)
 - IP Protocol > (IP Protocol Filters)
 - IP Port > (IP Port Filters)
- Ethernet Advanced > (Ethernet Advanced)
- AP Radio > (AP Radio Port)
 - Set Properties > (AP Radio Hardware)
 - Service Set ID (SSID) more > (AP Radio Service Sets)
 - Restrict Searched Channels > (AP Radio Restrict Searched Channels)
 - VLAN Setup > (VLAN Setup)
 - Radio Data Encryption (WEP) > (AP Radio Data Encryption)
 - VLAN Setup > (VLAN Setup)
- AP Radio Identification > (AP Radio Identification)
 - Service Set ID (SSID) more > (AP Radio Service Sets)
- AP Radio Hardware > (AP Radio Hardware)
 - Service Set ID (SSID) more > (AP Radio Service Sets)
 - Restrict Searched Channels > (AP Radio Restrict Searched Channels)
 - VLAN Setup (VLAN Setup)

- Radio Data Encryption (WEP) > (AP Radio Data Encryption)
 - VLAN Setup (VLAN Setup)
- AP Radio Hardware > (AP Radio Hardware)
- Service Set ID (SSID) more > (AP Radio Service Sets)
- Restrict Searched Channels > (AP Radio Restrict Searched Channels)
 - VLAN Setup (VLAN Setup)
- Radio Data Encryption (WEP) > (AP Radio Data Encryption)
 - VLAN Setup (VLAN Setup)
- AP Radio Filters > (AP Radio Protocol Filters)
 - Ethertype > (Ethertype Protocol Filters)
 - IP Protocol > (IP Protocol Filters)
 - IP Port > (IP Port Filters)
- AP Radio Advanced > (AP Radio Advanced)
 - Quality of Service Setup > (Quality of Service)
 - VLAN Setup > (VLAN Setup)
 - Advanced Primary SSID Setup > (AP Radio Primary SSID)

Figure A-6 Summary Status Event Logs Menu Tree

- Summary Status Logs > (Event Log)
 - Download Event Log > (File Download)
 - Additional Display Filters > (Event Display Setup)
 - Severity > (Event Log Summary)
 - Warning > (Even Log (Warning) Help)
 - Info > (Event Log (Info) Help)



Protocol Filter Lists

The tables in this appendix list the protocols available on the Protocol Filters pages described in the “Protocol Filtering” section on page 5-2. The tables include:

- Table B-1, Protocols on the Ethertype Filters Page
- Table B-2, Protocols on the IP Protocol Filters Page
- Table B-3, Protocols on the IP Port Protocol Filters Page

In each table, the Protocol column lists the protocol name, and the Additional Identifier column lists other names for the same protocol. You can type either name in the Special Cases field on the Filter Set page to select the protocol. Table B-3 also lists the protocols’ ISO numeric designators. You can use these designators to select a protocol also.

Table B-1 Protocols on the Ethertype Filters Page

Protocol	Additional Identifier	ISO Designator
ARP	—	0x0806
RARP	—	0x8035
IP	—	0x0800
Berkeley Trailer Negotiation	—	0x1000
LAN Test	—	0x0708
X.25 Level3	X.25	0x0805
Banyan	—	0x0BAD
CDP	—	0x2000
DEC XNS	XNS	0x6000
DEC MOP Dump/Load	—	0x6001
DEC MOP	MOP	0x6002
DEC LAT	LAT	0x6004
Ethertalk	—	0x809B
Appletalk ARP	Appletalk AARP	0x80F3
IPX 802.2	—	0x00E0
IPX 802.3	—	0x00FF
Novell IPX (old)	—	0x8137
Novell IPX (new)	IPX	0x8138
EAPOL (old)	—	0x8180
EAPOL (new)	—	0x888E
Telxon TXP	TXP	0x8729
Aironet DDP	DDP	0x872D
Enet Config Test	—	0x9000
NetBUI	—	0xF0F0

Table B-2 *Protocols on the IP Protocol Filters Page*

Protocol	Additional Identifier	ISO Designator
dummy	—	0
Internet Control Message Protocol	ICMP	1
Internet Group Management Protocol	IGMP	2
Transmission Control Protocol	TCP	6
Exterior Gateway Protocol	EGP	8
PUP	—	12
CHAOS	—	16
User Datagram Protocol	UDP	17
XNS-IDP	IDP	22
ISO-TP4	TP4	29
ISO-CNLP	CNLP	80
Banyan VINES	VINES	83
Encapsulation Header	encap_hdr	98
Spectralink Voice Protocol	SVP Spectralink	119
raw	—	255

Table B-3 Protocols on the IP Port Protocol Filters Page

Protocol	Additional Identifier	ISO Designator
TCP port service multiplexer	tcpmux	1
echo	—	7
discard (9)	—	9
systat (11)	—	11
daytime (13)	—	13
netstat (15)	—	15
Quote of the Day	qotd quote	17
Message Send Protocol	msp	18
ttytst source	chargen	19
FTP Data	ftp-data	20
FTP Control (21)	ftp	21
Secure Shell (22)	ssh	22
Telnet	—	23
Simple Mail Transport Protocol	SMTP mail	25
time	timserver	37
Resource Location Protocol	RLP	39
IEN 116 Name Server	name	42
whois	nickname 43	43
Domain Name Server	DNS domain	53
MTP	—	57
BOOTP Server	—	67
BOOTP Client	—	68
TFTP	—	69

Table B-3 *Protocols on the IP Port Protocol Filters Page (continued)*

Protocol	Additional Identifier	ISO Designator
gopher	—	70
rje	netrjs	77
finger	—	79
Hypertext Transport Protocol	HTTP www	80
ttylink	link	87
Kerberos v5	Kerberos krb5	88
supdup	—	95
hostname	hostnames	101
TSAP	iso-tsap	102
CSO Name Server	cso-ns csnet-ns	105
Remote Telnet	rtelnet	107
Postoffice v2	POP2 POP v2	109
Postoffice v3	POP3 POP v3	110
Sun RPC	sunrpc	111
tap ident authentication	auth	113
sftp	—	115
uucp-path	—	117
Network News Transfer Protocol	Network News readnews nntp	119
USENET News Transfer Protocol	Network News readnews nntp	119
Network Time Protocol	ntp	123

Table B-3 *Protocols on the IP Port Protocol Filters Page (continued)*

Protocol	Additional Identifier	ISO Designator
NETBIOS Name Service	netbios-ns	137
NETBIOS Datagram Service	netbios-dgm	138
NETBIOS Session Service	netbios-ssn	139
Interim Mail Access Protocol v2	Interim Mail Access Protocol IMAP2	143
Simple Network Management Protocol	SNMP	161
SNMP Traps	snmp-trap	162
ISO CMIP Management Over IP	CMIP Management Over IP cmip-man CMOT	163
ISO CMIP Agent Over IP	cmip-agent	164
X Display Manager Control Protocol	xdmcp	177
NeXTStep Window Server	NeXTStep	178
Border Gateway Protocol	BGP	179
Prospero	—	191
Internet Relay Chap	IRC	194
SNMP Unix Multiplexer	smux	199
AppleTalk Routing	at-rtmp	201
AppleTalk name binding	at-nbp	202
AppleTalk echo	at-echo	204
AppleTalk Zone Information	at-zis	206
NISO Z39.50 database	z3950	210
IPX	—	213

Table B-3 *Protocols on the IP Port Protocol Filters Page (continued)*

Protocol	Additional Identifier	ISO Designator
Interactive Mail Access Protocol v3	imap3	220
Unix Listserv	ulistserv	372
syslog	—	514
Unix spooler	spooler	515
talk	—	517
ntalk	—	518
route	RIP	520
timeserver	timed	525
newdate	tempo	526
courier	RPC	530
conference	chat	531
netnews	—	532
netwall	wall	533
UUCP Daemon	UUCP uucpd	540
Kerberos rlogin	klogin	543
Kerberos rsh	kshell	544
rfs_server	remotefs	556
Kerberos kadmin	kerberos-adm	749
network dictionary	webster	765
SUP server	supfilesrv	871
swat for SAMBA	swat	901
SUP debugging	supfiledbg	1127
ingreslock	—	1524
Prospero non-privileged	prospero-np	1525
RADIUS	—	1812

Table B-3 *Protocols on the IP Port Protocol Filters Page (continued)*

Protocol	Additional Identifier	ISO Designator
Concurrent Versions System	CVS	2401
Cisco IAPP	—	2887
Radio Free Ethernet	RFE	5002



Channels, Power Levels, and Antenna Gains

This appendix lists the channels supported by the world's regulatory domains as well as the maximum power levels and antenna gains allowed per domain.

This appendix covers these topics:

- Channels, page C-2
- Maximum Power Levels and Antenna Gains, page C-3

Channels

The channel identifiers, channel center frequencies, and regulatory domains of each 22-MHz-wide channel are shown in Table C-1.

Table C-1 Channels

Channel Identifier	Frequency	Regulatory Domains				
		Americas (-A)	EMEA (-E)	Israel (-I)	China (-C)	Japan (-J)
1	2412 MHz	X	X	-	X	X
2	2417 MHz	X	X	-	X	X
3	2422 MHz	X	X	X	X	X
4	2427 MHz	X	X	X	X	X
5	2432 MHz	X	X	X	X	X
6	2437 MHz	X	X	X	X	X
7	2442 MHz	X	X	X	X	X
8	2447 MHz	X	X	X	X	X
9	2452 MHz	X	X	X	X	X
10	2457 MHz	X	X	-	X	X
11	2462 MHz	X	X	-	X	X
12	2467 MHz	-	X	-	-	X
13	2472 MHz	-	X	-	-	X
14	2484 MHz	-	-	-	-	X
Maximum Power (mW)		100	100	100	5	50



Note

France may use 2412-2452 MHz up to 10 mW eirp, and 2457-2472 up to 100 mW eirp.
Mexico may use 2400-2483.5 MHz up to 650 mW eirp (2400-2450 for indoor use only).

Maximum Power Levels and Antenna Gains

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table C-2 indicates the maximum power levels and antenna gains allowed for each regulatory domain.

Table C-2 Maximum Power Levels Per Antenna Gain

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
-A Channel Set (4 watts EIRP maximum)	0	100
	2.2	100
	5.2	100
	6	100
	8.5	100
	12	100
	13.5	100
	21	20
-E Channel Set (100 mW EIRP maximum)	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1

Table C-2 Maximum Power Levels Per Antenna Gain (continued)

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
-I Channel Set (100 mW EIRP maximum)	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1
-C Channel Set (10 mW EIRP maximum)	0	5
	2.2	5
	5.2	n/a
	6	n/a
	8.5	n/a
	12	n/a
	13.5	n/a
	21	n/a
-J Channel Set (10 mW/MHz EIRP maximum)	0	50
	2.2	30
	5.2	30
	6	30
	8.5	n/a
	12	n/a
	13.5	5
	21	n/a



INDEX

A

access point creating and configuring VLANs on **4-11**

Access Point Radio Port page **13-12**

accounting on RADIUS server **9-15**

activity timeout **7-18, 9-8**

administrator authorization **8-41**

Aironet extensions **3-23**

antenna gains **C-3**

antennas **3-18**

Apply button **17**

AP Radio Advanced page **3-20**

AP Radio Hardware page **3-12**

AP Radio Identification page **3-9**

assigning network ports **9-13**

associations allowed, more than 20 workgroup bridges **3-23**

Association table

Association Table Advanced page **7-16**

Association Table page **9-2**

Station page **9-3**

authentication server

Authentication Server Setup page **8-21**

backup servers **8-40**

EAP **8-5**

port setting **8-22**

shared secret **8-22**

authentication types

combining MAC-based and EAP **8-34**

LEAP **8-24**

MAC-based **8-29**

Network-EAP **8-4**

open **8-7**

shared key **8-8**

summary of settings **8-37**

B

backup authentication servers **8-40**

basic settings

configuration server protocol **3-3**

default gateway **3-4**

ensure compatibility with **3-7**

IP address **3-4**

IP subnet mask **3-4**

optimize radio network for **3-7**

role in radio network **3-5**

SNMP admin. community **3-7**

SSID **3-4, 3-11, 3-13**

system name **3-3**

baud rate **21**
 beacons, period and rate **3-16**
 bit-flip attack **8-3**
 blinking top panel indicators **13-40**
 boot block version **13-45**
 BOOTP protocol **7-5**
 BOOTP server timeout **7-5**
 Boot Server Setup page **7-4**
 broadcast SSID **3-13**
 broadcast WEP key rotation **8-18**
 browsing to network devices **9-2**

C

Cancel button **17**
 carrier test **13-4**
 centralized administrator authentication **8-45**

- assigning RADIUS or TACACS servers **8-46**
- procedure for configuring **8-45**

 channel

- identifiers, center frequencies **C-2**
- overlap **3-17**
- restrict searched channels **3-17**
- search for less-congested channel **3-17**

 checkstack command **13-24**
 China regulatory domain **C-2**
 Cisco Secure ACS

- enabling EAP **8-25**
- setting session-based WEP key timeout **8-26**

CLI

auto-apply **23**
 common functions **22**
 diagnostics **13-19**
 terminal emulator settings **20**
 client devices

- browsing to **9-2**
- deauthenticating **9-10**
- disassociating **9-10**
- EAP settings **8-24**
- in network map **19**
- Station page information **9-4**

 cold restart **10-17**
 combining EAP and MAC-based authentication **8-34**
 configuration

- distributing the configuration **10-11**
- downloading the configuration **10-13**
- resetting the configuration **10-16**
- System Configuration Setup page **10-12**
- uploading the configuration **10-14**

 configuration server protocol **3-3**
 Console/Telnet Setup page **11-5**

D

Database Query page, gets and sets **11-3**
 data rate, radio **3-14**
 defined **11-6**
 DHCP

- class identifier **7-7**
- lease duration **7-5**
- minimum lease duration **7-6**
- multiple-offer timeout **7-5**
- diagnostic pages
 - AP Radio Port page **13-12**
 - Ethernet Port page **13-9**
 - Event Log page **13-16**
 - Network Ports page **13-6**
 - packet tracing **13-32**
 - Radio Diagnostics page **13-2**
- Disallow Infrastructure Stations **3-23**
- distribute configuration **10-11**
- distribute firmware **10-9**
- diversity, antenna **3-18**
- DNS server **7-9**
- draft of 802.1x protocol **8-21**
- DTIM **3-16**

E

- EAP authentication
 - combining with MAC-based authentication **8-34**
 - overview **8-4**
 - Require EAP setting **8-23**
 - setting up in Cisco Secure ACS **8-25**
 - setting up on the access point **8-20**
 - setting WEP key timeout **8-26**
- EIRP, maximum **C-3 to C-4**

- encryption. See WEP
- ensure compatibility with **3-7**
- Ethernet configuration
 - advanced settings **3-34**
 - hardware settings **3-31**
 - identity settings **3-28**
 - speed **3-32**
- Ethernet encapsulation type **3-24**
- Ethernet indicator **13-38**
- Ethernet Port page **13-9**
- Event Log page **13-16**
- Event notification
 - Event Display Setup page **7-18**
 - Event Handling Setup page **7-21**
- Express Setup page **3-2**
- extended statistics **7-18**

F

- filters
 - ISO numeric designators for protocols **B-1**
 - MAC address filtering **5-6**
 - protocol filtering **5-2**
 - protocol filter lists **B-1**
- find an access point's physical location **13-40**
- firmware
 - distributing to other Access Points **10-9**
 - menu tree **A-1**
 - updating to a new version **10-2**

flow control **21**
 fragment threshold **3-16**
 frequencies **C-2**
 FTP **7-10**

G

gateway **3-4**

H

help, setting up **7-7**
 hexadecimal digits **8-16**
 Home button **17**
 hops **9-7**
 Hot Standby mode **12-6**
 HTTP Port **7-8**
 HyperTerminal **23**

I

initialization vector **8-16**
 IP subnet mask **3-4**
 ISO designators for protocols **B-1**
 Israel regulatory domain **C-2**

J

Japan

power levels and antenna gain **C-4**
 regulatory domain **C-2**

K

key features **1-2**
 key hashing, WEP **8-16**
 Kilomicroseconds, in beacon period **3-16**

L

LEAP
 enabling on a repeater access point **8-27**
 with Network-EAP setting **8-19**
 LED indicators
 Ethernet **13-38**
 locate unit by flashing LEDs **13-40**
 radio traffic **13-38**
 status **13-38**
 link test **9-8**
 load balancing **3-23**
 locate unit by flashing LEDs **13-40**
 logs **13-16**

M

MAC address **3-3**
 MAC address filters **5-6**
 MAC-based authentication **8-29**

- combining with EAP **8-34**
- setting up in Cisco Secure ACS **8-35**
- map windows **18**
- memory, conserving **7-18**
- memory use diagnostics **13-28**
- menu tree **A-1**
- Mexico, regulatory domain **C-2**
- MIC **8-14**
- monitored access point **12-6**
- multicast packets **3-21**

N

- name server **7-9**
- NAS, adding and configuring **8-25**
- Native VLAN
 - configuration **4-5**
- native VLAN
 - creating **4-11**
- Network-EAP **8-4**
- network infrastructure, classify workgroup bridges as **3-23**
- network map window **19**
- Network Ports page **13-6**
- North America and ANZ regulatory domain **C-2**

O

- OK button **17**

- optimize radio network for **3-7**

P

- packet tracing **13-32**
- parity **21**
- password reset **13-43**
- pings **9-8**
- ports, assigning to MAC addresses **9-13**
- power level
 - maximum **C-3 to C-4**
- power level setting **3-15**
- preamble **3-28**
- primary port **3-10**
- protocol filters
 - enabling filters **5-5**
 - forward or block **5-5**
 - list of available protocols **B-1**
 - priorities **5-5**
 - time to live setting **5-4**
- Proxy Mobile IP **6-1**
 - components of **6-3**
 - configuring **6-19**
 - how it works **6-4**
 - security **6-8**
 - understanding **6-2**
- PSPF **7-18**

Q**QoS configuration 5-10**entering information for **5-10**example **5-17**Generate QBSS Element **5-11**Send IGMP General Query **5-12**settings on QoS setup page **5-11**Traffic Category **5-12**Use Symbol Extensions **5-11****Quality of Service**defined **1-5**

R**radio**carrier test **13-3, 13-4****radio cell role 3-22****radio configuration**advanced settings **3-19**hardware settings **3-11**identity settings **3-8**primary port **3-10****radio indicator 13-38****radio modulation 3-27****radio power level 3-15****RADIUS-based VLAN access control 4-6****RADIUS server**backup servers **8-40**shared secret **8-22**wireless network accounting **9-15**receive and transmit **3-18**receive antenna **3-18**

regulatory

domains **C-2**regulatory domains **C-2**related publications, obtaining **xviii**

repeater

chain of access points **12-3**setting up a repeater **12-2**setting up as a LEAP Client **8-27**specified access points **3-27**Require EAP setting **8-23**resetting to the default configuration **13-43**restarts, cold and warm **10-17**restore defaults **17**restrict searched channels **3-17**roaming **1-4**

rogue AP

alert timeout for **7-17**role in radio network **3-5**root unit **3-5**routing setup **7-11**RS-232 serial port **20**RTS retries and threshold **3-16**

S

search for less-congested channel
 restrict searched channels **3-17**

Secure Shell **11-6**

Secure Shell,using **11-6**

security
 Cisco Secure ACS **8-25**
 overview **8-2**
 Security Setup page **8-42**
 user manager **8-41**

serial cable **20**

serial number, system **3-29**

server setup
 boot server **7-4**
 FTP **7-10**
 name server **7-9**
 routing **7-11**
 time server **7-2**
 web server **7-7**

session-based WEP key, timeout value **8-26**

severity levels **7-17**

shared key **8-7**

SNMP
 Admin. community **3-7**
 Database Query page **11-3**
 SNMP Setup page **11-2**
 supported MIBs **25**
 using to set WEP **8-13**

Speed setting **3-32**

SSH **11-6**

SSID **3-4**
 primary and secondary **4-6**

SSID for use by Infrastructure Stations **3-23**

standby mode **12-6**

Station pages **9-3**

statistics **9-10**

status indicator **13-38**

stop bits **21**

system name **3-3**

T

Telnet interface
 enabling Telnet **11-6**
 setup page **11-5**

temporal key integrity protocol **3-26**

terminal emulator **20**

TFTP **7-11**

timeout per device class setting **7-18**

timeout value for session-based WEP keys **8-26**

time server
 GMT offset **7-3**
 manually set date and time **7-3**

TKIP **8-16**

top panel indicators **13-37**

tracing packets **13-32**

transmit antenna **3-18**

transmit power **3-15**

U

unicast packets, filtering **5-9**

updating firmware **10-2**

user management

capabilities **8-43**

creating list of authorized users **8-42**

user information **8-42**

using **11-6**

V

vendor class identifier **7-7**

VLAN configuration

802.1Q Encapsulation Mode **4-3**

broadcast domain segmentation **4-5**

creating and configuring on access point **4-11**

creating and configuring SSIDs **4-15**

creating native VLAN **4-11**

creating SSID for infrastructure devices **4-19**

enabling VLAN (802.1Q) tagging **4-17**

entering information **4-2**

example of **4-9**

Existing VLANs **4-4**

identifying the native VLAN **4-17**

Maximum Number of Enabled VLAN
IDs **4-3**

native VLAN configuration **4-5**

Native VLAN ID **4-3**

obtaining and recording setup
information **4-10**

Optionally allow Encrypted packets on the
unencrypted VLAN **4-4**

primary and secondary SSIDs **4-6**

rules and guidelines for **4-19**

security policy **4-4**

settings on VLAN setup page **4-2**

Single VLAN ID which allows Unencrypted
packets **4-3**

using configuration screens **4-10**

VLAN (802.1Q) Tagging **4-3**

VLAN ID **4-4**

VLAN Name **4-4**

VLANs

creating and configuring on access point **4-11**

creating and configuring SSIDs for **4-15**

creating native VLAN **4-11**

creating SSID for Infrastructure devices **4-19**

criteria for wireless deployment **4-8**

deployment example **4-9**

guidelines for deploying wireless **4-8**

Summary of rules for deployment of **4-19**

using configuration screens **4-10**

VLAN support

defined **1-6**

W

warm restart **10-17**

Web-based interface

- common buttons **17**

- compatible browsers **16**

Web server **7-7**

WEP

- broadcast key rotation **8-18**

- full encryption **8-12**

- key example **8-11**

- key hashing **8-16**

- key size **8-11**

- optional **8-12**

- overview **8-3**

- session key timeout **8-26**

- setting with SNMP **8-13**

- transmit key **8-11**

- with EAP **8-4**

Windows XP, using EAP with **8-21**

workgroup bridges, allowing more than 20 to
associate **3-23**

World mode **3-14**

